USE OF SOCIAL SECURITY NUMBER AS A NATIONAL IDENTIFIER

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SECOND CONGRESS

FIRST SESSION

FEBRUARY 27, 1991

Serial 102-11

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
43-544⇆ WASHINGTON : 1991

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

H781-38.

COMMITTEE ON WAYS AND MEANS

DAN ROSTENKOWSKI, Illinois, *Chairman*

SAM M. GIBBONS, Florida
J.J. PICKLE, Texas
CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ANDY JACOBS, Jr., Indiana
HAROLD E. FORD, Tennessee
ED JENKINS, Georgia
THOMAS J. DOWNEY, New York
FRANK J. GUARINI, New Jersey
MARTY RUSSO, Illinois
DON J. PEASE, Ohio
ROBERT T. MATSUI, California
BERYL ANTHONY, Jr., Arkansas
BYRON L. DORGAN, North Dakota
BARBARA B. KENNELLY, Connecticut
BRIAN J. DONNELLY, Massachusetts
WILLIAM J. COYNE, Pennsylvania
MICHAEL A. ANDREWS, Texas
SANDER M. LEVIN, Michigan
JIM MOODY, Wisconsin
BENJAMIN L. CARDIN, Maryland
JIM McDERMOTT, Washington

BILL ARCHER, Texas
GUY VANDER JAGT, Michigan
PHILIP M. CRANE, Illinois
DICK SCHULZE, Pennsylvania
BILL GRADISON, Ohio
BILL THOMAS, California
RAYMOND J. McGRATH, New York
ROD CHANDLER, Washington
E. CLAY SHAW, Jr., Florida
DON SUNDQUIST, Tennessee
NANCY L. JOHNSON, Connecticut
JIM BUNNING, Kentucky
FRED GRANDY, Iowa

Robert J. Leonard, *Chief Counsel and Staff Director*
Phillip D. Moseley, *Minority Chief of Staff*

Subcommittee on Social Security

ANDY JACOBS, Jr., Indiana, *Chairman*

SAM M. GIBBONS, Florida
BENJAMIN L. CARDIN, Maryland
JIM McDERMOTT, Washington
J.J. PICKLE, Texas

JIM BUNNING, Kentucky
PHILIP M. CRANE, Illinois
DICK SCHULZE, Pennsylvania

CONTENTS

Page

Press release of Thursday, February 14, 1991, announcing the hearing 2

WITNESSES

U.S. Department of Health and Human Services, Social Security Administration, Hon. Gwendolyn S. King, Commissioner of Social Security 20

American Civil Liberties Union, Janlori Goldman 114
Associated Credit Bureaus, Inc., D. Barry Connelly 82
Baskin, Roberta, Washington, D.C 89
Center for Immigration Studies, David Simcox 139
Computer Professionals for Social Responsibility, Marc Rotenberg 61
Connelly, D. Barry, Associated Credit Bureaus, Inc 82
Culnan, Mary J., Washington, D.C 91
Eaton, Joseph W., Pittsburgh, Pa 32
Federation for American Immigration Reform (FAIR), Daniel A. Stein 146
Goldman, Janlori, American Civil Liberties Union 114
Hendricks, Evan, Privacy Times 98
Martinez, Hon. Matthew G., a Representative in Congress from the State of California 10
Munoz, Cecilia, National Council of La Raza 130
National Council of La Raza, Cecilia Munoz 130
Rotenberg, Marc, Computer Professionals for Social Responsibility 61
Rothfeder, Jeffrey, Wyckoff, N.J 71
Simcox, David, Center for Immigration Studies 139
Simpson, Hon., Alan K., a U.S. Senator from the State of Wyoming 4
Smith, Robert Ellis, Privacy Journal 43
Stein, Daniel A., Federation for American Immigration Reform (FAIR) 146
Warfel Associates Inc., George H. Warfel, Sr 53
Wiggins, James R., Jr., Washington, D.C 78

SUBMISSIONS FOR THE RECORD

Center for Immigrants Rights, Jon Blazer, statement 162
Congressional Hispanic Caucus, Hon. Solomon P. Ortiz, Chairman, and a Representative in Congress from the State of Texas, statement 168
Linden, Larry F., Woodbine, Md., statement 169
National Association of Health Data Organizations, Mark H. Epstein, statement and attachments 171
North Texas Immigration Coalition, Jonathan Bernstein, statement 177
Organization of Chinese Americans, Inc., Daphne Kwok, statement 180
Roybal, Hon. Edward R., a Representative in Congress from the State of California, statement 182
Torres, Hon. Esteban E., a Representative in Congress from the State of California, statement 183

USE OF SOCIAL SECURITY NUMBER AS A NATIONAL IDENTIFIER

WEDNESDAY, FEBRUARY 27, 1991

House of Representatives,
Committee on Ways and Means,
Subcommittee on Social Security,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10 a.m., in Room B-318, Rayburn House Office Building, Hon. Andy Jacobs, Jr. (chairman of the subcommittee) presiding.

[The press release announcing the hearing follows:]

FOR IMMEDIATE RELEASE
THURSDAY, FEBRUARY 14, 1991

PRESS RELEASE #2
SUBCOMMITTEE ON SOCIAL SECURITY
U.S. HOUSE OF REPRESENTATIVES
1102 LONGWORTH HOUSE OFFICE BLDG.
WASHINGTON, D.C. 20515
TELEPHONE: (202) 225-9263

ANDY JACOBS, JR. (D., IND.), CHAIRMAN, SUBCOMMITTEE ON SOCIAL SECURITY, COMMITTEE ON WAYS AND MEANS, U.S. HOUSE OF REPRESENTATIVES, ANNOUNCES A HEARING ON THE USE OF THE SOCIAL SECURITY NUMBER AS A NATIONAL IDENTIFIER, ON WEDNESDAY, FEBRUARY 27, 1991, AT 10:00 A.M., IN ROOM B-318, RAYBURN HOUSE OFFICE BUILDING

Andy Jacobs, Jr. (D., Ind.), Chairman of the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, announced today that the Subcommittee will hold a hearing on the use of the social security number as a national identifier. The hearing will be held on Wednesday, February 27, 1991, beginning at 10:00 a.m., in room B-318, Rayburn House Office Building. Oral testimony before the Subcommittee will be limited to invited witnesses only.

BACKGROUND

The nine-digit social security numbering system was developed in 1935 in order to record and retrieve accurately the earnings records of workers. The creation of a identifying number that was unique to each worker prompted fears that, by placing the government in the business of gathering information on individuals, the government would ultimately become a police state tracking a worker's race, religion, and family history. Some politicians and newspapers warned against creating such a number.

Attempting to dispel these concerns, the first regulation issued by the Social Security Board declared that social security numbers would be used solely for social security purposes.

Recognizing the benefits of using one identifying number for many purposes, President Franklin Roosevelt signed an executive order which permitted Federal agencies to use the social security number for identification purposes. Government use of the social security number has expanded over the last 55 years. The number has become the identifying number for all individual taxpayers and their dependents age 1 year or older, military personnel and civil service workers. In addition, by law, a variety of Federal benefit programs require individuals to provide their social security number as a condition of receiving benefits. The Federal government also requires that social security numbers be provided by those buying a U.S. Savings Bond or opening a bank account.

State and local governments are permitted to use the social security number to administer any tax, general public assistance, vehicle registration laws, and to issue drivers licenses.

In recent years, some advocates of immigration control have suggested expanding the mission of the Social Security Administration to require the agency to serve as a quasi-identification bureau by matching names and social security numbers for employers. In addition, some have urged the creation of a national identification card as a means of preventing illegal aliens from obtaining work. One proposal would require the development of a counterfeit resistant social security card. A more elaborate proposal would require each state to modify its current drivers licenses to include the social security numbers accompanied by an electronic finger print or a biometric facial picture.

The extensive use of computers has resulted in the wide-spread private sector use of the social security number as an identifier. Many merchants require a customer to provide a social security number as a condition of doing business. Credit bureaus use the social security number to maintain individual credit files and routinely sell this information to almost anyone who requests it. The ability of the

(MORE)

private sector to gather information such as credit history, grocery store purchases, medical records, (including pre-natal information), family medical histories and genetic makeup has raised fears that in the near future unregulated companies will serve as national identity bureaus collecting and dispersing an individual's most private information.

At present, information bureaus generally operate in an uncoordinated manner using separate data bases to gather and disseminate information. Privacy experts have expressed concern about the ability of individuals to protect their personal privacy should these data bases be merged to form one large information network.

SCOPE OF THE HEARING

The hearing will focus on: the proposal to create a national identification card; how the social security number is currently being used to collect and disperse information about individuals; and means of protecting individual privacy rights in the computer age.

Invited witnesses have been asked to testify on the following issues:

* The arguments for and against creating a national identification card;

* The ability of existing and future technology to identify individuals and collect and disperse information about them, especially utilizing the social security number;

* The appropriate role of the Social Security Administration in providing information relating to the social security number;

* Whether private companies should be permitted to sell the social security number;

* Whether current privacy protections for the social security number and other data are adequate.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Persons submitting written statements for the printed record of the hearing should submit six (6) copies by the close of business Thursday, March 14, 1991, to Robert J. Leonard, Chief Counsel, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth Office Building, Washington, D.C. 20515. If those filing a written statement for the record of the printed hearing wish to have their statements distributed to the press and the interested public at the hearing, they may provide additional copies for this purpose to the Subcommittee, room B-316 Rayburn House Office Building, on the day of the hearing.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All statements and any accompanying exhibits for printing must be typed in single space on legal-size paper and may not exceed a total of 10 pages.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. Statements must contain the name and capacity in which the witness will appear or, for written comments, the name and capacity of the person submitting the statement, as well as any clients or persons, or any organization for whom the witness appears or for whom the statement is submitted.

4. A supplemental sheet must accompany each statement listing the name, full address, a telephone number where the witness or the designated representative may be reached and a topical outline or summary of the comments and recommendations in the full statement. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the Members, the press and the public during the course of a public hearing may be submitted in other forms.

* * *

* * * *

Chairman JACOBS. The hearing this morning of the Subcommittee on Social Security is on the proposition of the use of Social Security numbers as a national identifying number.

I would like to announce at the outset that our cochairman, Mr. Bunning of Kentucky, is not present on account of his attending the funeral of John Sherman Cooper, surely one of the greatest statesmen in the history of our country. And Mr. Bunning—I do not think he sends his apologies, because nobody would ever have to apologize for attending the services of such a great person.

We are honored and pleased to have two Members of the Congress in our first panel, first Hon. Alan Simpson of Wyoming and then Hon. Matthew Martinez of California, States that are out there somewhere.

Senator, welcome to the committee.

STATEMENT OF HON. ALAN K. SIMPSON, A U.S. SENATOR FROM THE STATE OF WYOMING

Senator SIMPSON. Chairman Jacobs, I thank you. We are out there somewhere, I promise you, although we are now the lowest in population of all the States in the Union, and I think my colleague, Congressman Martinez, represents the largest now. But the problem is going to be the same, whether it is a big State or a little State, and you are very kind to let me come by for a minute and take this opportunity to discuss my interest in preventing the use of fraudulent documents in the United States.

The wide availability of these fraudulent identity and work authorization documents is causing us some very real problems in America—not just in immigration, which is my particular curse that was visited upon me back in 1980 for reconstitution of a committee of the Senate Judiciary Committee that had been moribund. Then Senator Kennedy had taken it under his own wing, and then I was given the duty of chairman and Ted was my ranking member, and he has been a great and supportive help to me from the beginning in most cases. There have been a few lapses here and there, but nevertheless.

But fraudulent documents are the things that are hindering our system of employer sanctions, and that is going to be a whole new debate on that one, because there are those that say employer sanctions are of the basis of discrimination, and yet some of the great civil libertarians of our time are those that embrace employer sanctions. That is another matter.

But we cannot deter the employment of illegal aliens unless we have employer sanctions and do something with fraudulent documents. The availability of these fraudulent birth certificates, Social Security cards, and drivers licenses is a significant loophole in the national policy of deterring illegal immigration by denying work authority to those persons who are illegally in the country.

And then we have the issue of firearms. And without getting into that volatile emotional issue, but in the criminal law area, fraudulent documents are also defeating our ability to prevent the sale of firearms to convicted felons and other persons forbidden by law to possess a weapon.

And whatever one's views are on gun control—and out in our part of the country, that simply means how steady you hold your rifle, I can tell you that—there is a consensus that criminals should not be able to possess weapons. I think we all believe that. But however, because of the widespread availability of fraudulent identity documents, birth certificates, and drivers licenses, a convicted felon can easily purchase firearms.

Terrorism, a whole new thing—I mean, not a new thing, but a new awareness of things, heightened in recent months because of the war in the Persian Gulf, the ability of those to use work authorization documents not only permits them to come illegally into the country and live here, but they permit terrorists to rent houses, set up bank accounts, purchase items on credit for their evil missions and numerous other activities.

If we want to address the problem of terrorism, we have to develop ways to improve the easily defeated system of documents.

So last year this subcommittee was included in last year's conference committee on the Immigration Act of 1990 and we are very pleased that we came out with a result. And you were very appropriate and forceful in objecting to a proposal for a pilot program agreed to by the Judiciary Committee members, however, in both the House and the Senate.

It would have done two things. It would have required State drivers license authorities to contact the Social Security Administration to match the Social Security number submitted by an applicant with the name for which that number was issued. It would require a few States to include biometric information on new drivers licenses.

The Social Security Administration has already tested programs that match a number to a name for which the number has been issued. In 1987, for the cities of Dallas, El Paso, and Corpus Christi, about 70,000 employers were able to match the numbers and names of Social Security cards by calling the Dallas Social Security Administration District Office. There were 23,000 Social Security numbers actually checked during a 1-year period. Now I cite that from "A New Role for the Social Security Card" in a General Accounting Office—GAO—report of March 1988.

While GAO did note some of the enforcement limitations to a telephone verification system, it made no mention of civil liberties complaints, problems or violations, none. Thus during the period of this telephone demonstration project, no civil liberties were infringed upon. A number of persons not authorized to work were detected, over 4,000 were detected, and Big Brother did not step up on the stage.

Then, under the provisions of the Tax Reform Act of 1976, States are authorized to use the Social Security number on drivers licenses, and the Social Security Administration has for years provided matching information to those States that requested it. My point is clear. The Immigration Act of 1990 was not proposing something new or even something untested. Name and number matching has already been done and is being done with little incident. And those who represented the pilot project in the immigration bill as a dramatic and sinister new proposal were absolutely incorrect.

Biometric data on identity documents will mean placing one's thumbprint on a drivers license. California, and hear this, is already considering doing this for all of its drivers license but it is already done on commercial drivers license in California; the requirement that biometric data be placed on commercial drivers licenses is already the law in California. The requirement was included in section 9105 of Public Law 100-690, the Anti-Drug Abuse Act of 1988.

So Congress has thus considered and approved requiring biometric identification information on certain drivers licenses; California is now considering the placement on all licenses. So as you see, Mr. Chairman, the proposal is neither novel nor without support. In fact, I would imagine most Members in the Congress have already voted for it. And that brings me to the conclusion that I thought the subcommittee took at last year's immigration bill conference. I was somewhat startled and puzzled, not offended, mind you, startled and puzzled, by this subcommittee's refusal to even discuss the Judiciary Committee's proposal on the merits.

All I heard—not from the chairman—was rhetoric about tattoos and national I.D. cards and complaints about changing the hallowed Social Security card on an immigration bill. And let me say and end that name and number matching has already been done, and biometric data requirements are now the law. So I trust we might have a discussion on the merits of this important issue. And I would love to engage in that, and we can start today, or on the floor, but many of those who are opposed to controlling illegal immigration use the specter of the national I.D. card.

I have been all through that. I have been in this stuff for 12 years. Any time they run out of facts here, you go to emotion, fear, guilt or racism, or xenophobia or you name it, it goes splattering off into all different directions. But never have we ever talked about a national I.D. card. It raises the emotional pitch, diminishes the careful consideration of proposals to make our documents more secure; something for the national interest.

It certainly happened last year during the House's first consideration of the conference report, and it worked. And rather than let a whole bill go down the tube, we made the adjustment and thanks to Chairman Joe Moakley of the Rules Committee, we were able to patch it all back together and get it done—something for the national interest.

But the specter of this has also crept into the subcommittee's press release on this hearing, where it says, "Some have urged the creation of a national identification card as a means of preventing illegal aliens from obtaining work."

I can say to you, sir, no Member, no Member of the Congress, to my knowledge, has ever proposed the creation of a national I.D. card. I do not support creation of a national identity card. The 1986 Immigration Reform and Control Act had an entire section in it which was just about as clear as you can get in our line of work, which is difficult, admittedly: "Nothing in this section shall be construed to authorize directly or indirectly the issuance or use of a national identification card or the establishment of a national identification card." That is the 1986 act.

The section goes on to talk about what is available, the privacy of information, to protect the privacy and security of personal information—not to be carried on the person, not to be used for law enforcement, restriction of due documents; that is the law.

So I hope that we can stop tossing around the rhetoric and start talking about the cold, hard specific issues, and let's look at the national interest. Do we want to make our State, Federal, and local documents less susceptible to fraud? Yes or no? Take your pick. Can we improve these documents without impinging on important civil liberties or creating a national I.D. card? Yes or no? But I hope we will not just slip back to emotion, fear, guilt, and racism, because I have had 12 years of that stuff in dealing with illegal immigration reform and now legal immigration reform, and it does not fit anything in my background whatsoever.

So I stand ready to cooperate with the chairman and any member and any committee or subcommittee to work on achieving this very difficult but very important task, which is something that I have been assisted in by people like Father Ted Hesburgh and Democrats and Republicans on both sides of the aisle for a goodly period of time. And I thank you for your courtesy and your attention, and I look forward to this discussion.

[The prepared statement follows:]

STATEMENT OF SENATOR ALAN K. SIMPSON

HEARING ON USE OF SOCIAL SECURITY NUMBER

SUBCOMMITTEE ON SOCIAL SECURITY

HOUSE COMMITTEE ON WAYS & MEANS

FEBRUARY 27, 1991

Mr. Chairman, and members of the Committee, I appreciate this opportunity to discuss my interest in preventing the use of fraudulent documents in the United States.

THE PROBLEM:
The wide availability of fraudulent identity and work authorization documents in our nation is causing our country serious problems in many areas.

Immigration: In the immigration context, fraudulent documents are hindering our system of employer sanctions from more effectively deterring the employment of illegal aliens. The availability of fraudulent birth certificates, social security cards, and drivers' licenses is a significant loophole to the national policy of deterring illegal immigration by denying work authority to those persons who are illegally in our country.

Firearms: In the criminal law area, fraudulent documents are also defeating our ability to prevent the sale of firearms to convicted felons and other persons forbidden by law to own or possess a weapon. Whatever one's views are on "gun control" -- and in my state, the definition of "gun control" is "a steady aim" -- there is a consensus that criminals should not be able to possess weapons. However, because of the widespread availability of fraudulent identity documents -- in this case, birth certificates and drivers' licenses -- a convicted felon can easily purchase a firearm.

Terrorism: we have properly heightened our concern about terrorism in recent months because of the war in the Persian Gulf. The widespread availability of fraudulent identity and work authorization documents not only permits potential terrorists to illegally enter the United States and live here, but these documents also permit terrorists to rent houses, set up bank accounts, purchase items on credit for their missions, and numerous other activities which could endanger the public safety.

Let there be no mistake: if we want to address the problem of terrorism in the United States in a serious manner, we have to develop ways to improve our easily defeated system of documents.

RECENT PROPOSALS:
This subcommittee was included in last year's conference committee on the Immigration Act of 1990 (Public Law 101-649). It objected to a proposal for a pilot program, agreed to by the Judiciary Committee conferees, that would have done two things: 1) required State driver's license authorities to contact the Social Security Administration to match a social security number submitted by an applicant with the name for which that number was issued, and 2) required a few States (in the pilot project) to include biometric information on new drivers' licenses. Let me discuss each in a little detail.

Social security number and drivers' licenses: the Social Security Administration has already tested programs that match a number to the name for which that number has been issued. In 1987, in the cities of Dallas, El Paso, and Corpus Christi, Texas, about 70,000 employers were able to match the numbers and names of social security cards by calling the Dallas Social Security Administration district office. 23,158 social security numbers were actually checked during a one-year period. (See Immigration Control: A New Role for the Social Security Card, General Accounting Office, March 1988, GAO/HRD-88-4.)

While GAO did note some of the enforcement limitations to a telephone verification system, it made no mention of civil liberties complaints, problems or violations. Thus, during the period of this telephone demonstration project, no civil liberties were infringed upon, a number of persons not authorized to work were detected (over 4,000), and "big brother" did not become a reality.

Under the provisions of the Tax Reform Act of 1976, states are authorized to use the social security number on drivers' licenses, and the Social Security Administration has for years provided matching information to those states that requested it.

My point is simple: the Immigration Act of 1990 was not proposing something new or even something untested. Name-and-number matching has already been done -- and is being done -- with little incident. Those who represented the pilot project in the immigration bill as a dramatic new proposal were absolutely incorrect.

Biometric data: placing "biometric data" on identity documents will mean placing one's thumbprint on a driver's license. California is already considering doing this for all of its drivers' licenses. In addition, the requirement that biometric data be placed on commercial drivers' licenses is already law. This requirement was included in § 9105 of Public Law 100-690, the Anti-Drug Abuse Act of 1988.

Congress has thus considered and approved requiring biometric identification information on certain driver's licenses, and California is now considering the placement of such information on all licenses. As you can see, this proposal is neither novel nor without support -- in fact, I imagine most members of the committee have already voted for it.

This brings me to the position taken by this subcommittee at last year's immigration bill conference. Frankly, I was somewhat puzzled by this subcommittee's refusal to discuss the Judiciary Committee's proposal on the merits. Let me re-emphasize: name and number matching has already been done, and biometric data requirements on some drivers' licenses are now the law. I look forward to a substantivediscussion on the merits of this important issue this year.

SCARE TACTICS BY OPPONENTS:

Many of those who are opposed to controlling illegal immigration use the spectre of a "national I.D. card" to raise the emotional pitch and diminish the careful consideration of proposals to make our documents more secure. This certainly happened last year, during the House's first consideration of the conference report on the Immigration Act of 1990. This spectre also snuck into this subcommittee's press release for this hearing, where the following statement was made: "...some have urged the creation of a national identification card as a means of preventing illegal aliens from obtaining work."

No Member of Congress, to my knowledge, has ever proposed the creation of a "national I.D. card." I do not support creation of a national identity card. The 1986 Immigration Reform and Control Act had a section which prohibited creation of a national identity card, both by specific prohibition and by substantive rules.

It is time for some advocates to stop throwing around the rhetoric and start talking about the cold, hard, specific issues. It is time to look at the national interest.

Do we want to make our federal, state and local documents less susceptible to fraud? Yes, we do.

Can we improve these documents without impinging on important civil liberties or creating a national identity card? Yes, we can.

I stand ready to cooperate with any Member and any committee in Congress to work on achieving this difficult but important task.

Chairman **Jacobs**. We thank you, Senator.

Mr. Martinez.

STATEMENT OF HON. MATTHEW G. MARTINEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. **Martinez**. Thank you, Mr. Chairman.

Let me start out by saying that I understand the Senator's desire. I think his desire is not too much different than many of us in Congress: to control immigration and to stop the fraudulent use of documents. But I think after that point, we disagree on how to achieve this.

As the Senator was speaking, I was thinking about the words in the preamble to the Constitution and why we established the Constitution. One reason was to ensure domestic tranquility. Yet, I do not see how we can ensure domestic tranquility when we in Congress pass laws that create fear. And fear, whether substantiated or not, is still fear.

I have always believed, even since we discussed IRCA, that a national identifying card will create discrimination. And I am not one that stands up and yells, "discrimination," or claims racism at the drop of a hat. I have never believed in it. I have been fortunate enough to escape heavy racism during my life and have been helped by people from other ethnic backgrounds. I know that there are a lot of people out there who are not racist and do not discriminate. But the reality is that every time we become so passive that we believe that discrimination is dead, it raises its ugly head again in some situation and we realize that it is not.

I do not believe that you can ever legislate away discrimination, but I do believe that you can legislate in such a way that discrimination is not done in public. The Government must protect people's rights. That is very important. I believe, like I have for a long time, that the agencies are not doing their job.

Let me relate to you some of my own personal experiences. I have visited several Social Security Offices in my district, found that they have the training to easily detect forgeries. They can detect forgeries of birth certificates and everything else. However, the employers, without training, are not able to detect a forged document.

There is a very simple method that when that payment starts coming in from the Social Security office to determine whether that is being used by the person, I think that is their responsibility to detect Social Security forgeries. I think it is inherent in the law when the Social Security Department says you must have a card for tax purposes, that only you and you alone can be issued this card, and only you can use it. I think that the agency can do more in the way of finding out who is using the numbers, since it is all computerized now. As the Senator said, there are States that have requested name and number matchup, and they have done it successfully. So it is not as if you are putting a burden on them that they cannot handle. They can do it. But why should the States have to request it or why should an individual employer have to request it? I think it should be done automatically when the first payment on a Social Security card comes in.

We are fearful of a national identity card, and we have come the closest to it we have ever been with the Social Security card. Now, at birth a person must have a Social Security number to be claimed as a dependent. But still, it is not a national identifier card. You can live in this country as a citizen or as a legal immigrant and not have one, if you do not work.

Thus there are a lot of reasons why you really do not need and why there has not been a national identifier card. The greatest fear we have is that this is a foot in the door. And that is a real fear. And as much as any reason, just because of the real fear, I am opposed to any system of national identifier, even a pilot program. In pilot programs, there is a tendency to take figures, the half-empty, half-full situation, and determine what they want to determine by those numbers and then report them that way. And we end up with a seemingly successful program. I am very worried of that.

I really believe that some in this country have become so paranoid about the invasion of America by illegal immigrants that we are willing to go to any lengths to stop that flow. There are better ways to confront this problem besides resorting to a national identifying card. One solution is to beef-up the borders. When you say the borders, most people tend to think of the southern border, and that is not a reality.

Illegal immigrants come in from ports, from Asia. They come in from the northern border also. In fact, the INS, did a raid in Denver, Colo., where they found that the illegals they picked up, 2 to 1, were not Hispanic but Anglo, coming in through the Canadian border from Europe. So we have to really stop thinking in narrow terms of where illegal immigration is coming from.

In the southwest, naturally because it is so close to the southern border, much of the illegal immigration comes from there. But I do not think we have ever tried establishing any kind of a work system as we have for H-2 for other industries that might be able to use this kind of labor. We can work with the other governments to make sure that this immigration is legitimate and that we know where they are and what they are doing and when they go back.

Let me relate another personal experience. I grew up in east L.A., where there is a predominance of people that have immigrated from the southern border, primarily from Mexico and in later years from the other South American countries. There was always a feeling from those people coming from Mexico that they only wanted to come here and make some money to send back to support their family in Mexico, because there was no economy there. They live a very, very poor life there.

And in doing this, they would have to go back occasionally and visit. When it got easier they would lead their families across rather than going back and forth between the United States and Mexico and risk being caught by the border patrol and sometimes abused. They decided that it was easier to just stay in the United States. But many of them always have had the idea that when they come here, they are going to go back some day.

I think if we made it easier for them to travel back and forth to work under a program like the H-2, we would eliminate that. The other aspect of it is helping them create an economy that keeps them there rather than bringing them here. All these things working together would go a long way to correct that problem.

I do not think you are ever going to stop people from wanting to come here because we provide freedom from oppression, political or economic. That is one of the attractions that this country holds. But I think that we can do it by strengthening the processes by which agencies can stop the fraudulent use of documents because they alone can do it.

Let me refer to something that I read several years back when the good Senator was interviewed by U.S. News and World Report. He stated the first document that an illegal alien gets is a drivers license since it is the easiest thing to obtain. Then with that drivers license, he goes on to get all kinds of documents providing his permanent residence here when, in fact, he has no permanent legal status.

And the Senator's comment in the article was, "I can't tell these forgeries from the real thing. How can the average employer?" And I think he is absolutely right. It is impossible for us to put that burden as we did in sanctions, on the employer, trying to make the employer, the INS officers, not requiring our other agencies such as the motor vehicle departments in the different States to make sure that the person applying for a drivers license is a legal resident. I understand that now they require that you provide some proof, a birth certificate, a passport or whatever it is, that proves your legal residence here, but let me tell you something, they are not doing the job they should do and that is why so many illegal immigrants slip through the cracks. If they would do more enforcing and more stringent, careful requirement of them providing the documents they need, we would eliminate a lot of this problem.

I am not so naive that I think that everything we do might eliminate all of the problems. They will not. There are still going to be some abuse. But we can eliminate a lot of this by enforcing these measures.

Mr. Chairman, the chairman of the Hispanic Caucus, Congressman Solomon Ortiz, has sent along a statement that he would have like to have read into the record, but I suppose that as long as it is included in the record that it would be sufficient.

Chairman JACOBS. Without objection.

Mr. MARTINEZ. I also have my written prepared text which I would like to submit for the record.

Chairman JACOBS. Well, I do not know about—well, yes, OK.

Mr. MARTINEZ. I really believe that before we start thinking in terms of a national identifying card, which scares the devil out of everybody, that we ought to think of enforcing other parts of the law that are not being carried out to the extent that should be. This would correct a lot of the problems that we have.

I would be willing to enter into discussion with Senator Simpson and the panel in trying to come to a proper solution for this problem.

[The prepared statement follows:]

STATEMENT OF THE HONORABLE MATTHEW MARTINEZ (D-CA)
MEMBER OF CONGRESS
BEFORE THE WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY

February 27, 1991

ALTHOUGH THERE IS LITTLE DOUBT THAT THE SOCIAL SECURITY NUMBER HAS SUCH WIDE SPREAD USAGE THAT IT IS ALREADY CONSIDERED BY MANY TO BE A NATIONAL IDENTIFYING NUMBER, THIS IS A MISNOMER AND SHOULD BE DISCOURAGED. NOTWITHSTANDING THE FACT THAT MOST PEOPLE HAVE SOCIAL SECURITY NUMBERS IN ORDER TO WORK, COLLECT SOCIAL SECURITY AND CLAIM CHILDREN ON THEIR TAXES, HAVING A SOCIAL SECURITY NUMBER IS DEFINITELY NOT THE SAME AS A NATIONAL IDENTIFYING NUMBER. IT IS NOT REQUIRED FOR LIVING IN THE UNITED STATES AS A NATIONAL IDENTIFYING CARD WOULD BE.

INSTEAD IT IS USED BY THOSE WHICH CHOOSE TO BE INVOLVED IN THE ABOVE MENTIONED PROGRAMS, AND RECEIVE THE BENEFITS OF MEDICARE, SOCIAL SECURITY, AND OTHER PROGRAMS FUNDED THROUGH TAXES. WE MUST KEEP IN MIND, HOWEVER, THAT THERE ARE SEGMENTS OF OUR SOCIETY, SUCH AS THE AMISH, WHERE MANY ARE SELF-SUFFICIENT AND ARE NOT EMPLOYED. THESE INDIVIDUALS ARE NOT REQUIRED TO HAVE A SOCIAL SECURITY NUMBER.

GEORGE ORWELL'S "1984" DEALT WITH THE INFAMOUS "BIG BROTHER" GOVERNMENT WHO WATCHED EVERY MOVE ITS' CITIZENS MADE. A NATIONAL IDENTIFYING NUMBER COULD BE THE BEGINNING OF AMERICA'S BIG BROTHER SYNDROME. THIS COUNTRY WAS FOUNDED ON THE BELIEF OF FREEDOM FOR ALL. EVEN THE STATUE ON TOP OF OUR CAPITOL BUILDING IS CALLED FREEDOM. ESTABLISHING A PERMANENT SYSTEM WITH A NATIONAL IDENTIFYING NUMBER WOULD DISRUPT THAT FREEDOM WHICH WE ALL CHERISH.

AS WE ALL KNOW, TODAY'S SOCIAL SECURITY NUMBER IS USED FOR SEVERAL MORE REASONS THAN ORIGINALLY INTENDED, AND I AM NOT SAYING THAT IT SHOULDN'T BE USED AS EMPLOYMENT VERIFICATION OR TO OPEN A BANK ACCOUNT, OR FOR MANY OTHER PURPOSES. WHAT WE NEED TO ADDRESS IS IMPROVING THE TECHNOLOGY TO PREVENT THE CONSTANT MISUSE OF THE SYSTEM.

MOST MEMBERS OF CONGRESS COULD TELL NUMEROUS STORIES OF HOW THEIR CONSTITUENTS WERE LEFT IN A QUANDARY WHEN THE SOCIAL SECURITY ADMINISTRATION MISTAKENLY GAVE OUT A DUPLICATE NUMBER TO ANOTHER APPLICANT; OR WHEN AN ILLEGAL ALIEN MADE UP A NUMBER WHICH A CONSTITUENT ALREADY HAD ISSUED TO THEM. THESE SITUATIONS ARE NOT UNCOMMON, BUT THEY SHOULD BE UNCOMMON AND AVOIDABLE. PEOPLE SHOULD NOT HAVE TO WORRY ABOUT WHETHER SOMEONE ELSE IS USING THE SAME NUMBER. THESE PEOPLE ARE OFTEN CHARGED FOR TAXES WHICH THEY DO NOT OWE ON EARNINGS THAT THEY DID NOT COLLECT.

THE SOCIAL SECURITY ADMINISTRATION HAS TO BE ABLE TO IMPROVE THEIR TECHNOLOGY IN ORDER TO PROTECT THE SOLE USER OF A SOCIAL SECURITY NUMBER. ALSO, SOCIAL SECURITY CARDS ARE PERHAPS ONE OF THE EASIEST TO FORGE. PERHAPS IF THEY WERE NOT JUST A FLIMSY PIECE OF PAPER WE COULD FORGO SOME OF THE PROBLEMS WE HAVE ENCOUNTERED WITH FORGED CARDS, AND MISREPRESENTATION OF NUMBERS.

IN CLOSING, LET ME STATE ONCE AGAIN THAT THE ESTABLISHMENT OF THE SOCIAL SECURITY NUMBER AS A NATIONAL IDENTIFYING NUMBER WOULD BE A GRAVE INJUSTICE TO THE PEOPLE OF THIS NATION. INSTEAD WE MUST CONCENTRATE ON PROVIDING THE SOCIAL SECURITY ADMINISTRATION WITH THE TOOLS NECESSARY TO MAINTAIN ACCURATE RECORDS AND TO PROTECT CITIZENS AGAINST THE POSSIBILITY OF FRAUDULENT USAGE OF THEIR SOCIAL SECURITY NUMBERS.

Chairman JACOBS. Thank you, Mr. Martinez, for your contribution to the record.

Mr. McDermott will inquire.

Mr. McDERMOTT. I am new to the committee, so I come here with more questions, ignorance, than anything else. One of the things that I recently read in the New York Times, which I guess I—it expands this whole question of using the Social Security number—a man had a son who was diagnosed with a genetic disease. The father was tested and the mother was tested for the genes for that genetic disease. The father shortly thereafter was found to be negative, as was the mother, for the gene—or the mother had the gene but the father did not—the father lost his auto insurance.

The auto insurance company had gotten that data, that medical data, and on the basis of the child's disease—the father did not even have the gene, but the child had the disease—the father was denied insurance because it was a genetic disease that controls the upper muscles of the arms and would make it impossible to drive.

As I read this kind of thing, these kinds of proposals, I see more ramifications in terms of insurance denials and all kinds of other things as that Social Security number becomes enmeshed in the whole system. And I am really more interested in those kinds of abuses—or do you consider that an abuse of the use of an identifier that is accessible to banks, insurance companies and everybody else who wants to get at it?

That is really my question to Senator Simpson.

My question is, does that concern you and how do you deal with the security issues?

Senator SIMPSON. Well I say to you, Congressman, that it certainly concerns us, and in the whole activity of doing immigration reform and having a lot of thoughtful Democrats and Republicans help me in the process, that is a very serious issue. But the anecdotal information you have just furnished me concerns me as a human being, but I do not think that is what we are particularly zeroing in here about.

We are talking about the Social Security card and matching, and whether this is new or novel or inappropriate, whether it can lead to discrimination. I really could not respond to what you have described, except that it is a terrible thing. But what we have been talking about from the beginning and what Father Ted Hesburgh talked about, who I consider one of the finest civil libertarians of our time, was that we need a more secure identifier system, one that is universally presented.

Please do not miss the aspect of this. This is not a document presented by people who look foreign. It is presented by bald Anglos like Simpson and it is presented at the time of new hire employment. That is when it is presented. And it says right in the law that it will not be used for law enforcement; it will not be used for any kind of other information; it is to be used at the time of new hire, and it is not to be carried on the person. All those things are in this bill, the 1986 law.

So what we are trying to do is this: As we know now, the border arrests are going up, and people are asking about terrorism; how in God's name do you do anything about terrorism in the United States unless you get to a better identifier system? For every anecdotal issue as you have described, I can show you another one of a person who came to this country, went into the system, got the drivers license, got the house, started up the operation and it is a serious detriment to our national interest.

Mr. McDermott. As I listen to this, I mean, I go back and forth across the border to Canada a lot. I go through the border that has the third highest travel at Blaine, Wash. Are you suggesting that every time I cross the border, I would have to present this?

Senator Simpson. No, no, I am talking about new hire. If you are talking about immigration and illegal immigration, that is what I was speaking of. I know it is difficult.

Mr. McDermott. If I am in a car and I say I am a resident and I live in Seattle, how do they know?

Senator Simpson. Well, you are presenting some kind of documents.

Mr. McDermott. You are not presenting any documents. You are just driving through in your car.

Senator Simpson. That is fine, you know, however it is done. I am not challenging that. I am not talking about that. We were trying to get a pilot program to match things up here so that we could deal with illegal immigration and issues that are ancillary to that, like terrorism, issues of criminals with guns, people with drugs.

California felt strongly enough about it to put this biometric requirement on their commercial drivers licenses, and that is—let's keep that in mind that they did that. People talk about well, if we would only beef up the border or if we would do law enforcement. Well, that is interesting, because when you do that, that is not satisfactory either, because that "impinges on rights." And then you have got to remember who is pressing for employer sanctions along with Al Simpson and some other Democrats, Republicans, the AFL–CIO.

You get all into these things of employer sanctions, identifiers, penalties. I even had in my bill—there were penalties for those employers who only checked particular applicants to be sure that we avoided discrimination. To me the ultimate discrimination is to be in this country and to be illegal and not have the rights that others have. That is my peculiar, twisted view of the whole issue.

Mr. Martinez. Might I respond?

Mr. McDermott. Sure.

Mr. Martinez. I understand the Senator's concern, especially in the area of fraudulent documents, which allow people who come into the country illegally to stay. And I understand his concern about the terrorists. You know, many of the terrorists, or the potential terrorists, come in legally. They come in very early on with the full intent that one day they will look for an opportunity to do terrorist acts.

We have allowed them to come in. I do not know how you prevent that from happening, since we do allow legal immigration. But one of the things that the Senator talked about was a biometric identifier. That scares the devil out of people. If it is a fingerprint, let's say fingerprint. I understand that they are talking about using a new system of fingerprinting and that is why they give it the terminology biometric.

But it scares people because biometric also includes brain scans and a lot of other things that people just are scared to death with. I have been in a Social Security office when illegals, not Hispanic illegals, Asian illegals came in with full sets of documents, birth certificates and everything else. They could not hardly speak the language. They made themselves understood. But the person behind the desk could tell and then looked very closely at these documents. The first thing they spotted was the new Social Security card, which is supposed to be forgery proof. Evidently it is because they could tell that that was a forgery.

Now I understand that the Social Security Department itself has a huge fund of moneys that are paid by illegals that will never be claimed. And I am wondering why we are not using that money for more enforcement.

But the point is that we can do the things that Senator Simpson wants to do, with what we have. Now, you are concerned about the misuse of a Social Security card. Nobody ever said in law that the banks could require it for you to identify your bank account, but evidently the banks are very comfortable that this is the best and safest way to identify that depositor.

That being the case, then I think we do not have to go any farther than how the Social Security now is used. But we must make sure that the person using that number is really entitled to use that number. I keep stressing that over and over again, because when I sat in those Social Security offices they assured me, at least in those local offices that they are detecting forgeries. If the committee wanted to have GAO do a study in the southwestern district or in places like Florida where there is a lot of immigration, they will find that those offices are, and the employers are not finding the forgeries and detecting them and stopping the use of them. And I think that the Social Security office is where it has to be done.

Mr. McDermott. But it turns out to be that there are not enough people in Social Security offices.

Mr. Martinez. And not enough money to automate for faster identification system.

Mr. McDermott. Thank you, Mr. Chairman.

Chairman Jacobs. Mr. Pickle.

Mr. Pickle. Mr. Chairman, thank you. I do not think I have any questions for the panel. I am particularly pleased though to hear the testimony of our colleague, Mr. Martinez, who is a recognized leader in the field of training and education and has a lot of practical experience in it.

I also am particularly pleased to welcome Senator Simpson here. The Senator from Wyoming has a well-earned reputation of not failing to invade where the angels fear to tread.

Senator Simpson. You ain't kidding. I have had it today.

Mr. Pickle. He likes to get at the heart of an issue, and he has got the courage to advance revolution in the area, with a lot of new ideas and recommendations. So I am delighted to see him here continuing his interest in this subject on which he and I both have worked.

I simply say to you, to both of you, particulary you, Senator Simpson, I am not sure that I know enough about the proposed biometric drivers license system. I think it could work, but I think it gets Social Security more and more into the business of identification, and the question is do we want to give them that burden?

In our zeal to administer a lot of governmental programs, the temptation is to use Social Security, and that is because it may be the only practical alternative to a lot of these perplexing problems we have. And our temptation is to do that. I would think, though, that we ought to be careful. If we want to get into the identification question, I personally think we probably ought to just meet head on the question of national identification, to establish one or not.

I question really whether we ought to do it through or with Social Security, because Social Security was established to keep wage records. It was not charged with the responsibility of the identification of illegal workers or immigration or food stamps. And I think that is so fundamental, that fact overshadows a lot of other temptations on my part.

But I do recognize that we are more and more on an annual basis using the Social Security card for more and more identification purposes. And the question is how far do we go or how much we want to saddle Social Security with, entering into this identification question? And for that fundamental question, we do not yet have an answer.

I think these hearings, Mr. Chairman, are good and I salute you for having them. It whets our interest and causes us to think about what can we do and how can we do it better? So I will be looking at your proposal more, Senator Simpson, and try and examine it. I just recommend your initiative, and I am glad to see you are here personally. We welcome you. Thank you.

Mr. MARTINEZ. Mr. Chairman, might I just make a statement?

Chairman JACOBS. Yes.

Mr. MARTINEZ. Mr. Pickle, I think I agree with you. I do not want to see the use of the Social Security card expanded, but it is being used to a great degree as an identifier for certain things. We know that. We cannot deny that. Those people have confidence in it, and that is why they use it.

The thing that I am saying is not expanding the use of it, but making sure that the person using it is entitled to use it and I think we can do that. I think the Social Security Administration itself has the capability of making sure that the person that uses the number is the one that is entitled to use it. I think just doing that eliminates the need for a national identification card.

Mr. PICKLE. Perhaps. But whatever system you use, you cannot prove anything more than that number represents that number and not that that person is the person we are trying to find. So you can talk all you want to, and you come up with the same unanswered question.

Senator SIMPSON. Chairman Jacobs, when I made my aside there, it was not about this committee. I had a pretty good load dropped on my head by one of the local publications this morning, and that is what I was speaking of, nothing more than that.

But you talk about profiles in courage, Jake Pickle, in honestly trying to deal with the Social Security system years ago, is just that I admired and I told him then, and I told him now, I think he was thinking, "Are you really encouraging me along, Simpson, so I can fall off this cliff all by myself?" I said, "No, no, I will stay with you," because he is honest about what must be done with that system in its benefit structure in the year 2030, and we owe that to our children and grandchildren. And my admiration for him goes way back.

Chairman JACOBS. Well Senator, Congressman Pickle is a little bit like Sarah Lee cakes; nobody doesn't like Jake. [Laughter.]

Senator, you mentioned the provision in the Immigration Act, the standard language nestling in this act shall not be construed to create a national identification number, and I suppose that brings up the question of the generic or the duck quacking theory of identification provisions.

But apparently, and I tend to agree with you, I think that nothing in this act, would purposely create a national identification number. The language almost is plain enough for a judge to understand. But I am just wondering how you would analyze then the administration's disposition toward the Civil Rights Act last year. The administration vetoed the act asserting that it created quota requirements, yet in the act was precisely that language, "Nothing in this Act shall be interpreted as requiring quotas."

Do you think the language was less efficacious there than it was in the Immigration Act or vice versa?

Senator SIMPSON. I have always desperately tried to separate anything I am doing with immigration or I ever did with it with civil rights. In fact, there was an amendment in the early immigration legislation in 1982 to make English the official language of the United States, which I voted against and which passed 76 to 24 in the most extraordinary array of Democrats and Republicans voting for it that you have ever seen.

And as far as the Civil Rights bill, all I know is that in my view, it would not have done anything more than lead an employer to advocate a quota simply because he would not have been able to meet the tests which was not a return to the *Griggs* decision. Whether they overturned *Wards Cove,* whatever they did, would have put the employer in a position so that to be safe he or she would have simply had to go to quotas, and I thought that was not appropriate. Regardless of the words or language—and I think many people, as they write about what happened, maybe we can do a bill this time which is honest and goes back to *Griggs,* even if you overturn *Wards Cove* and get something which does not force employers into doing a quota just to protect themselves.

Chairman JACOBS. Well, by coincidence, as I understand it, that is precisely what people are worried about in the employer sanction area of the immigration legislation. No matter what it says, "Nothing in this Act shall require," in practice and in effect, employers would err on the side of staying on this side of the bars and would, perforce, and I say perforce, not by disposition, end up discriminating against Hispanics.

So almost the same practical concern seems to apply to both situations. I do not say this in criticism. I think it delineates the dilemma with which we are faced. It is not a simple thing to solve. Bill Malden did a cartoon one time where a little boy made a report in school and said, "So my conclusion is that war is impossible unless both sides is right," and that is what produces an issue, of course.

And I think on behalf of the subcommittee, or what is left of it——[Laughter.]

Senator SIMPSON. Where is Jake when we need him?

Chairman JACOBS [continuing]. We do want to express our gratitude, because you have enriched the record. As you indicated, there was hardly the opportunity, a mega-conference meeting at the closing of the Congress with Jack Brooks this time—eyes upon Texas, as I recall—to discuss this thoroughly. And I think this is a more relaxed circumstance, and we are very grateful for your contribution, and Matt, we are grateful for your contribution as well. And we appreciate your willingness to serve on this same panel or testify in the same panel because it is a great way to narrow things down, I think, so.

Senator SIMPSON. Ask my friend about the California commercial drivers license, though, because it has a biometric thumbprint right on it.

Mr. MARTINEZ. This is what I said earlier. You know, the idea of just referring to biometric identification scares the devil out of people. We are used to thumbprints. A while back, a few years back, even before they put the photograph on, they had a thumbprint on it. And so, when the people went back to it, they were not really alarmed. But they would have been more alarmed if somebody would have told them you are going to now be required to have a biometric identifier on your drivers license, because immediately they conjure up future, scientific kinds of experimental testing of your brain waves and other things because they have seen it in all the sci-fi movies and books where that is what they talk about when they talk about a biometric identifier.

Chairman JACOBS. Well, Matt, as you probably know, and you do not know, Senator, I am a former police officer. I have found that it is not unusual for those who are not well-positioned in society to run from the police even though they are thoroughly innocent. So there is that apprehension about authority with which one has to contend, I think.

Senator SIMPSON. Having been on Federal probation for shooting mailboxes, I remember the feeling. [Laughter.]

Thank you, and I appreciate you inviting us. And you have a reputation for astuteness and good humor and——

Chairman JACOBS. Most people just stop at the word reputation. [Laughter.]

Senator SIMPSON. Thank you.

Mr. MARTINEZ. We appreciate it very much.

Chairman JACOBS. Our next panel, and I think, without objection, we will apply the 5-minute rule now for testimony. We have quite a long list of witnesses and it is not very fair to the people down at the whip end of the witness line if we consume too much time—I mean, after the Commissioner, the 5-minute rule will apply. I wish it did not have to apply anyplace, but once we get into the private witnesses, we usually apply it. So you can speak for 2 or 3 hours, Ms. King. [Laughter.]

STATEMENT OF HON. GWENDOLYN S. KING, COMMISSIONER OF SOCIAL SECURITY, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Ms. KING. Thank you, Mr. Chairman. I would like to submit my full written statement for the record and make some brief opening remarks and in fact they will be very brief since Mr. Pickle has pretty much delivered the full text of my oral testimony.

Chairman JACOBS. Without objection.

Ms. KING. As you examine the Social Security number and its current uses, I intend to outline for you, as requested, the original purpose of the Social Security number, the ways in which use of the number has expanded in the last 30 years, and how that expanded use has affected the Social Security Administration—SSA. I will also describe our current disclosure policy. First, some history.

In the 55 years since the Social Security Act was passed, SSA has issued roughly 350 million Social Security numbers. As you know, this nine-digit Social Security numbering system was designed as an administrative means by which to keep track of the earnings of people who work in jobs covered under the new program.

Its sole original purpose, and it was a narrow purpose, was to indicate that a unique number had been issued to an individual and to provide employers with the proper Social Security number for reporting earnings for their employees. In fact, since this was its only original purpose and since SSA initially was pressed to issue some 30 million numbers in a very short period of time, it was decided early on that the numbers would be issued based only on a person's statements, whether documented or not, about his or her name, date of birth, and other identifying information.

That, of course, has changed in recent years. Legislation was passed in 1972 to make our documentation requirements more stringent. But in spite of the new stricter documentation requirements, I must emphasize, Mr. Chairman, that the majority of the Social Security number records today, over 60 percent, still are based on the assertions a person made at the time he or she applied for a Social Security number. That, of course, means that the Social Security number simply cannot be used effectively as a means of identification.

And yet today it is widely used for non-Social Security purposes in both the public and private sectors. This expanded use was hastened by the computer revolution in the 1960s which combined with the simplicity of using a unique number that most people had already been issued, provided the major impetus for widespread use of Social Security numbers.

In 1961, the Federal Civil Service Commission began using the SSN as an identifying number for all Federal employees. In 1962, the IRS decided to use it as its taxpayer identification number for individuals. Then, in 1967, the Defense Department adopted the Social Security number as its identification number for military personnel. Later that use expanded to State and local governments and to the private sector, to banks and credit bureaus, hospitals, and educational institutions, for use in their computer and other recordkeeping systems.

Now, although both the public and private sectors are using the number, the expanded use of the Social Security number in the public sector has generally been under specific statutory authority. The first explicit statutory authority to issue Social Security numbers also came in 1972 as a result of congressional concerns about welfare fraud and aliens working in the United States illegally.

Legislation was passed that year requiring Social Security to issue numbers to all legally admitted aliens authorized to work in this country and to take affirmative steps to issue Social Security numbers to individuals applying for or receiving any Federal benefits.

Subsequent Congresses have enacted legislation requiring a Social Security number as a condition for eligibility for aid to families with dependent children benefits, food stamps, the school lunch program, and Federal loan programs. And, in 1976, States were authorized to use the number in the administration of taxes and general public assistance and in conjunction with their drivers' license or motor vehicle registration laws. In recent years, other legislation has allowed the use of the Social Security number for draft registration, commercial motor vehicle operators licenses and other uses.

This expanded use of the Social Security number has affected us in the area of verification. We are asked by third parties to verify that the name and Social Security number in their files matches those in our Social Security number records, and where we are required by law and in certain circumstances where we are permitted by law to do so, we comply with these requests.

We do such verifications primarily through our regular automated exchanges with Federal and State needs-tested benefit programs to help ensure the accuracy of their eligibility determinations. However, with the exception of employers for wage reporting purposes, Social Security does not verify Social Security numbers for the private sector because of limits we have established in our disclosure policy to protect the privacy rights of our Social Security number holders, and to limit the use of our resources to the business of Social Security.

I must say this. Expanded use of the Social Security number could become very burdensome for us if proposals were adopted to make the Social Security card a national identifier, if we can use that expression. The process of verifying identities and reissuing every American a new, more secure card could be very costly, in the range of $1.5 to $2.5 billion. Of course, the exact cost would depend on the exact security features built into such a card. But it would, in any case, require an enormous diversion of our attention and resources from our program responsibilities. And clearly, we do not have those resources at this time.

Beyond the immense practical problems for such a proposal, Social Security has historically had fundamental concerns about the potential for invasion of privacy under such proposals, particularly if all records pertaining to an individual could be accessed under one number. And that brings me to our disclosure policy and under what circumstances do we give out information about individuals.

Our disclosure policy was developed and refined over the years to protect individual privacy rights as best we can within our purview. An individual's Social Security number is the key to accessing a variety of information about that individual. That fact has shaped our current policy. Therefore, our policy is this: we do not disclose information about an individual without his or her consent unless we are required by the statute to do so or unless there are reasons to do so related to the administration of the Social Security program or of other governmental health or income maintenance programs.

In conclusion, Mr. Chairman, use of the Social Security number has expanded far beyond its original purpose of keeping track of earnings for individual workers. If this use continues, Mr. Chairman, we would like to believe that we would continue to be responsible for protecting the privacy of individuals. We are very concerned about the potential harm to individuals through careless use of a number.

We would be happy to work very closely with this subcommittee as you examine the issue.

[The prepared statement follows:]

TESTIMONY OF GWENDOLYN S. KING
COMMISSIONER OF SOCIAL SECURITY

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today as you focus attention on how the Social Security number is being used to collect and dispense information about people, and on ways to protect individual privacy in the computer age.

As you requested in your letter of invitation, I will discuss the original purpose of the Social Security number, or SSN as we call it, and how its use has expanded over the years. I will then describe what effect this expansion has had on the Social Security Administration (SSA) and the conditions under which we disclose or verify an SSN for third parties.

Original Purpose of the Social Security Number and Card

Following the passage of the Social Security Act in 1935, the SSN was devised administratively as a way to keep track of the earnings of people who worked in jobs covered under the new program. The requirement that workers covered by Social Security apply for an SSN was published in Treasury regulations in 1936. (Treasury issued this requirement because it was given general authority by law to implement the taxation provisions of the Act.)

Initially, the only purpose of the Social Security card was to indicate that a number had been issued to an individual and to provide an employer with the proper SSN for reporting earnings for an employee. Primarily because some 30 million numbers had to be issued in a very short time, a decision was made that SSNs should be issued based on a person's statements (whether documented or not) about his name, date of birth, and other identifying information. This procedure was sufficient early on because at that time the SSN's sole purpose was to provide an individually unique number for recording wages reported for workers.

Growth of SSN as an Identifier for Non-SSA Purposes

In spite of the narrowly drawn purpose of the SSN, use of the SSN as a convenient means of identifying people in records systems has grown over the years. In 1943, Executive Order (EO) 9397 required Federal agencies to use the SSN in any new system for identifying individuals. This directive had no significant, immediate effect on use of the SSN. Instead, it was the computer revolution which took hold in the 1960's--and the simplicity of using a unique number that most people already had been issued--that provided the major impetus for widespread use of the SSN by Government agencies and private organizations.

In 1961, the Federal Civil Service Commission established a numerical identification system for all Federal employees using the SSN as the identifying number. The next year, the Internal Revenue Service (IRS) decided to use the SSN as its taxpayer identification number (TIN) for individuals. And, in 1967, the Defense Department adopted the SSN as its identification number for military personnel. In the following years, use of the SSN for computer and other recordkeeping systems spread throughout State and local governments, and to banks, credit bureaus, hospitals, educational institutions and other areas of the private sector.

Statutory Expansion of SSN Use

The first explicit statutory authority to issue SSNs did not occur until 1972, when Congress required that SSA issue SSNs to all legally admitted aliens authorized to work in this country and take affirmative steps to issue SSNs to children and anyone receiving or applying for a benefit paid for by Federal funds. This change was prompted by congressional concerns about welfare fraud and about aliens working in the U.S. illegally. Subsequent

Congresses have enacted legislation which requires an SSN as a condition of eligibility for AFDC benefits, Medicaid, food stamps, the school lunch program, and loans under any Federal loan program. Also, States were authorized in 1976 to use the SSN in the administration of any tax, general public assistance, driver's license or motor vehicle registration law within their jurisdiction.

Separate pieces of legislation in recent years have provided for additional uses of the SSN including draft registration, commercial motor vehicle operators' licenses, and for operators of stores that redeem food stamps.

Evidentiary Requirements for SSNs

Not surprisingly, as public and private use of the SSN expanded, so too did congressional concern about the integrity of the SSN. In 1972, Congress enacted Social Security legislation to tighten the SSN evidentiary requirements. Thus, SSA's regulations contain the following requirements for SSNs:

- All applicants--regardless of age--are required to provide documentary evidence of age, identity, and U.S. citizenship or alien status. Generally, for a new SSN, an applicant must submit at least two forms of acceptable evidence. For example, an adult U.S. citizen can use a birth certificate and a driver's license, and an alien can use a birth certificate and an immigration record; and,
- A personal interview is conducted with all SSN applicants aged 18 and older who apply for new numbers. This is primarily because it is unusual for people living in the United States not to have an SSN by age 18.

Let me emphasize, Mr. Chairman, that because these more stringent documentation requirements were not implemented until the late 1970's, the majority of SSN records today--over 60 percent--still are based on the representations that were made by the numberholder at the time he or she applied for an SSN.

Effect on SSA of Expanded Use of SSNs

The largest non-Social Security use of SSNs in the public sector is for income tax purposes. In recent years, we have issued SSNs as TINs to millions of children age 2 and older who are claimed as dependents on Federal tax returns. Also, the 1990 Omnibus Budget Reconciliation Act requires that children over age 1 must have SSNs in order to be claimed as dependents on returns for tax year 1991.

Expanded use of the SSN also has led to requests for SSA to verify that the name and SSN in the files of third parties are the same as those on our SSN records. Where required by law and, in certain circumstances where permitted by law, we comply with SSN verification requests. Such verifications are done primarily through our regular automated exchanges with Federal and State needs-tested benefit programs to help ensure the accuracy of their eligibility determinations.

Except for employers to report wages, SSA does not verify SSNs for the private sector because of limits we have established in our disclosure policy to protect the privacy rights of SSN holders and to limit use of our resources to the business of Social Security.

Expanded use of the SSN through proposals to make the Social Security card a national personal identifier could create a tremendous burden for SSA. The current Social Security card is of no use as a personal identifier because it contains only a name, an SSN, and a space for a signature after the card is received by mail. Thus, anyone can fraudulently present a Social Security card issued to another person.

Even if the Social Security card were enhanced to make it more effective as a personal identifier, there still would be a problem of ensuring that the card had been properly issued to an individual. This is because the documents an SSN applicant must present to establish identity--primarily birth certificates--are relatively easy to alter, counterfeit, or obtain fraudulently.

Let me mention, too, what an enormous and expensive undertaking it would be to issue new Social Security cards containing enhancements to make them useful for personal identification. The process of verifying identities and reissuing everyone a new, more secure card would be very costly--in the range of $1.5 to $2.5 billion. The exact cost would depend on the security features and issuance procedures used, but in any case reissuance would require an enormous diversion of SSA attention and resources from our program responsibilities.

Also, SSA and the Congress have historically had fundamental concerns about the possibility that the SSN might become a universal identifier in this country. These concerns center on questions of individual privacy and the increased possibility of the invasion of that privacy if all records pertaining to an individual could be accessed under one number. While no one advocates such a step, we must be careful that the SSN does not become a de facto national identifier, particularly in record systems.

SSN Disclosure Policy

Our policy regarding disclosure of SSNs reflects our concern about maintaining the privacy of information regarding individuals in SSA records. Thus, our policy is not to disclose information about an individual without his or her consent unless we are required by statute to do so, or there are reasons to do so related to the administration of the Social Security program or of other governmental health or income maintenance programs.

Conclusion

Mr. Chairman, use of the SSN has expanded far beyond its original purpose of keeping track of earnings for individual workers. The expanded use by Federal and State programs has generally been under specific statutory mandate.

The need for a unique number for individual records in computer systems means that use of the SSN is likely to continue to expand in the years ahead. While the Social Security Administration is not, and we believe should not be, responsible for use of the SSN in the private sector, we have a deep concern that individuals not be harmed through carelessness in the use of the SSN.

We will be happy to work closely with the subcommittee as you examine the many uses of the Social Security number.

Chairman JACOBS. Thank you very much. Mr. McDermott will inquire.

Mr. McDERMOTT. My only question is what percent of your time is spent in offices over the Nation verifying these numbers?

Ms. KING. I do not have that percentage at my fingertips.

Mr. McDERMOTT. Or how many inquiries do you have in a year?

Ms. KING. We get a number of inquiries. Let me give you just some basic facts on where our numbers currently are. In 1990, fiscal year 1990 alone, we issued 19 million Social Security cards, 9,150,000 of which were original cards, first-time issuances. So for each of those new cards, we had to verify the information. There were 9,850,000 replacement cards and of course we do require some information in order to replace cards.

Mr. McDERMOTT. Do you go through and fully verify?

Ms. KING. On the original?

Mr. McDERMOTT. On a replacement card?

Ms. KING. On replacement cards, we do not fully verify. Someone comes in and says, "My Social Security number is this and this is my name," and they give us some basic information. We require them to show us some documentation.

Mr. McDERMOTT. Can they do it by mail?

Ms. KING. We have a form called the SS-5, and people fill out the form and are required to send that in to us. We can pretty much in 2 to 3 weeks time send them a replacement card.

Mr. McDERMOTT. There would be no way you would know if somebody died, somebody got a hold of a card, and sent the data in——

Ms. KING. In the case where someone dies, we have ongoing matching arrangements with the various States to plug in information about when someone does die, and we plug that in immediately. So, if someone shows up to try to get a replacement card, we go in through the system, and the system immediately kicks out the fact that this person has died.

Now, that works very well most of the time. Sometimes, unfortunately, there is a mixup in numbers, and I ran into this when I was out in Grand Island, Nebr. The first thing I ran into was a gentleman who said to me, "Why did Social Security kill me?" I said, "Please, sir, I just arrived. Can you just explain what we did to you?" It turns out that he had the exact same name as someone else and he got a letter from us that was generated by our computer system saying——

Mr. McDERMOTT. Sorry to hear that you died?

Ms. KING [continuing]. To his wife, saying, "I'm sorry your husband died. We are going to take your recent check we deposited and so forth." So every now and then, we have a glitch. But I think it is healthy for us to fess-up firsthand, because I am sure you hear about those that do happen. Those are very rare.

Mr. McDERMOTT. If I am an employer and I have an employee that I kind of wonder about and I send in the Social Security number, will you verify it for me and tell me this is the person?

Ms. KING. Generally speaking, Mr. McDermott, I think we ought to be clear on what we will verify. If you are hiring someone and you have a Social Security card and you want to know if this Social Security number that we have in our files in fact matches the number there that you are presenting, we will tell you. Keep in mind that all we could ever tell you anyway is whether the name and Social Security number are the same.

We do not know what you look like. There is no picture. There is no identifier on our Social Security cards. So the question of whether it is a helpful personal identifier is clear—it's limited. It is of limited value. It goes to the heart of the question of what happens if I give my cousin who wants to get a job and does not have a Social Security number—what happens if I loan her my Social Security number? It means that my cousin will be paying into my Social Security account and she is not going to be getting any benefits under her own name. So I am not really sure how helpful our verification is.

But I think Mr. Martinez was correct in his observation that when people do bring documents to us, our Social Security employees are very astute in picking up fraudulent documents and identifying documents that have been altered, and they have very clear instructions of what to do in those circumstances. If they pick up a document that has been altered, they confiscate it on the spot, depending on how safe the circumstances are. We also provide copies of fraudulent documents to the appropriate officials who need to have them.

Mr. McDERMOTT. How many benefit checks do you send overseas?

Ms. KING. Benefit checks overseas?

Mr. McDERMOTT. My question really is directed at how many documents or how many numbers are floating around in the world while you deliver benefit checks? When I was in the State Department, one of the consular officer's jobs was going up in the bush and delivering checks to people all over the place.

Ms. KING. We now have Federal benefit officers out in seven locations around the world who often go out and check. One of the things we do is sort of automatically trigger when people get to a certain age. We started with age 100 and we are working our way down. We actually go out and eyeball people to say, "Hi, just wanted to make sure you are doing OK and thought I would stop by to see you." If for some reason someone dies in a foreign country and that country or consular officers fail to notify us of that event, there could be a situation where we continue to spew out the checks.

The first time we did that, I think the first time since I was Commissioner about a year ago, and that information came to me, we really had scrubbed down the numbers pretty much. We cut out a good deal of the potential for fraud by just going out and eyeballing people on the spot.

Mr. McDERMOTT. Thank you.

Chairman JACOBS. Mr. Pickle will inquire.

Mr. PICKLE. Thank you, Mr. Chairman. Ms. King, I am sorry. I was not here to hear your comments.

Chairman JACOBS. Why don't you ask her what she said?

Ms. KING. I began, Mr. Pickle, by saying that you had in fact already given my oral statement because our main purpose here is ensuring the privacy of the people who have Social Security numbers, protecting their wage information. And the reason that we got this system going so quickly was, in fact, to provide a method of recording that wage data; so you had already given my approach.

Mr. PICKLE. Well, let me ask you on behalf of the Social Security Administration, under what circumstances would Social Security share SSA information with a private employer in any circumstance?

Ms. KING. We do not, Mr. Pickle, generally disclose information. We do release information, under certain circumstances, for verification of a number; that is, if an employer is trying to hire someone and wants to make sure that the number and the name match. But remember, our Social Security cards do not have a picture on them. There is no way for us to identify that person for the employer, which is, I think, often very confusing to people.

We do not disclose any information for non-Social Security purposes. So when an employer comes to us and is planning to hire someone and wants to verify the name and number before they start to pay taxes in to Social Security on behalf of that employee, we can confirm that we have the same name and number for the name and number they present to us. Again, we are not in a position to say whether or not that person standing there is a person that we can match up with the name.

Mr. PICKLE. Well, Social Security, within the past few years, did actually give information to the employers, did actually furnish information to private employers, and you may do it now to a very limited extent. Are you out of the business of giving information out to employers, identification numbers?

Ms. KING. I think, Mr. Pickle, you may be referring to the fact that some time ago, Social Security was also providing information about people to people who were not interested in them for employment purposes, for paying their Social Security taxes. We are out of that business, as you know. The *Reporters* decision made it very clear that we will not disclose information to private sector people just for their convenience. We are no longer doing anything like that.

Mr. PICKLE. Well, have you investigated the possibility of issuing any kind of a card, trying to establish an ID card in connection with the Social Security program?

Ms. KING. Again, part of the problem that we would be faced with is the fact that we have some 250 million active Social Security numbers today and about 60 percent of them were issued prior to the time when we were required to get additional pieces of documentation. Remember, when we started the program, we very quickly issued those 35 million-or-so cards without requiring a birth certificate or without requiring some other documentation.

So we really, Mr. Pickle, are in the business of keeping our records for purposes of Social Security. We are riveted on trying to make sure that our process works for people who pay into the system so that we can pay benefits accurately. And we do not want to get into the business of being the national identifier. I don't think Social Security should be in that business.

Mr. PICKLE. Now, have you got a study with respect to any kind of a cost that would be involved if you were asked to produce a card for identification? Would it be an expensive problem for you?

Ms. KING. Absolutely. And there is no question about that. There are a couple of options that people have asked us to consider, such as whether we could have a plastic card or some kind of card with one of those magnetic strips on the back. Somebody said, well, how about a card with a hologram? As you know, on your credit cards, it is that fancy little sparkly thing. I don't know that that would mean anything to the 65,000 employees at Social Security. We don't have the wherewithal to recognize a thumbprint, for instance. But surely, we know that the plastic cards will cost us anywhere from 15 cents to $1.50 depending on what you put on it. When you figure that we have 250 million cards to reissue, we are talking about anywhere from $1.5 to $2.5 billion.

Mr. PICKLE. Earlier the Senator from Wyoming suggested a biometric drivers license type of card. I know that that would be expensive and if you use a plastic card we know that that would be very expensive. And that still doesn't settle the question of if the person who holds that card is that person? So we could have a lot of expense.

The real problem, I guess, is that if you have some kind of a card imposed on you, I would assume that would be an extra burden on Social Security to administer.

Ms. KING. Absolutely.

Mr. PICKLE. And, if you did, you would be getting away from the basic purpose, which is keep the records for wage credits only.

Ms. KING. Absolutely.

Mr. PICKLE. That was why it started. So that every worker, at the end of his working years, knows that he gets credit for the wages that he has earned and based on that, his Social Security figure is determined. And that is really the only thing.

Now, practically speaking many Government agencies use it for different purposes. And I can understand that, and there is a growing nagging recognition, I think, on the part of the public, that we need to have more information. Somehow we ought to try to match up these people, but in the course of it, I would say you would come back and say Social Security, you do it. And I hesitate to say that is your responsibility. If we are going to get into that ID card business, we ought to just say, shall we have a nationalized ID card and just wade right into the question.

But I would rather think that we ought not to do it from a Social Security standpoint, I never have.

Ms. KING. I couldn't agree with the gentleman more. I think, Mr. Pickle, you have absolutely identified the issue. I think that it can be very frightening when you think about how private the information about your wages and what you earn has to be for every individual. I think it would be a tragic mistake for us to move in the direction of not being in control of what the Social Security card and number can be used for.

Right now, we know that our records are protected, that we do not let that information out to anyone. As I say, it is as much as we can do to manage that accurately so that we can pay benefits accurately.

Mr. PICKLE. And already we have seen the Social Security card being used and proliferated in a manner that that information is getting perilously close to being a disclosure of basic rights and information, particularly in the health field and credit informant field. These ID cards, I mean Social Security numbers are being "sold" now by credit groups and other organizations and they pass that on to the other individual and it affects his earning ability or his health rights.

So, I think that we have got to be very careful before we do this thing.

Ms. KING. I agree.

Mr. PICKLE. I thank you, Mr. Chairman.

Chairman JACOBS. Mr. Gibbons will inquire.

Mr. GIBBONS. Thank you, Mr. Chairman.

Ms. King, you made an excellent statement and I can understand your desire not to become any more greatly involved in trying to secure records and things of that sort. But don't you think, as a practical matter, we are eventually going to evolve in our society to some kind of national identification card or number?

Ms. KING. Well, as a practical matter, we may be moving in that direction, but I would submit to you, Mr. Gibbons, that it is probably not in the direction of having Social Security hold the reins there. It just seems to me that we can talk about fingerprints and holograms and magnetic strips and all of those other kinds of identifiers, but one thing that seems to work well for everybody on a driver's license is a photograph. And you get that renewed every so often. So as you get these gray hairs, they show up in the picture. I don't know if there are many circumstances where most of us go through the day that somebody doesn't say, can I see a driver's license or a credit card?

Maybe that's the direction that we ought to be moving in. But when you realize that 30 States use the Social Security number on the driver's license, that causes me some consternation. It makes me want to redouble my efforts to protect the Social Security records, the earnings records, that really is my charge. I think that we need to avoid at all costs giving people wholesale access to that information.

Mr. GIBBONS. No doubt about that. No doubt about that.

You know, yes, I have spent millions of dollars identifying myself to about 600,000 people over 38 years. [Laughter.]

Millions of dollars, bill-boards and everything else, television ads, and yet, although I am constantly in my own constituency, I am constantly asked "Can I see some kind of identification, sir?" And I always get out whatever I have, usually a credit card, but they usually always want my Social Security number.

I think de facto we have just moved into something that we didn't really intend to get into, probably foresaw in 1935, that we are going to have a national identification card. Even if some entrepreneur has to begin selling them because maybe that is the way we will do it. Let some private company set up—not let them, I guess they could now sell a national identification card if they wanted to—but it seems that we are going to do it.

And I don't want to get you into the business of disclosing information on individuals, but I am afraid that your card number has already become the national identification number, even with the defects that you have within the system, that it is a self-proclaimed system.

So I don't know where we are going in all of this. I think we ought to be very careful about having to give out information and particularly earnings records. But it looks like to me we are already in a national identification crisis and we are meeting it one way or another.

Ms. KING. Well, I would suggest though, Mr. Gibbons, that until such time as the law requires that people show their Social Security number, it is not a national identifier, and now the law does not require anyone to show his or her Social Security card to anyone.

Mr. GIBBONS. If I want to buy something or want something and somebody wants to see my identification, I should be able to tell them to go to hell if I wanted to and walk out. I never have done that.

Ms. KING. I know. I would not have a driver's license today if I had done that, even though I was inclined to do it.

Mr. GIBBONS. No, but I don't think we ought to be required to do that, but it looks like to me that we are moving into some kind of national identification program. I don't know what it is going to be. Maybe it is going to be your system.

Mr. PICKLE. Will the gentleman yield?

Mr. GIBBONS. Sure, I will yield you some.

Mr. PICKLE. Mr. Chairman, I just wanted to add that Ms. King just stated that there was a time, just a few years ago that Social Security did actually sell or give information to private business. And that has been discontinued and you do not carry that practice on.

I don't suppose though that there is anything that would keep you from starting that up again next month if you wanted to?

Ms. KING. There is the Supreme Court ruling in *Reporters,* Mr. Pickle, that would certainly keep me from doing it.

Mr. PICKLE. Well, you may have a Supreme Court ruling that touches on the subject. I am not so sure of that, but we ought to put in the law that you can't do it. And that's a little bit more direct than a court decision that might touch on the things generally. So I think, Mr. Chairman, that we might even go take the affirmative.

Chairman JACOBS. We thank you for your testimony, Ms. King. It just struck my mind, I think sometimes as many as 15 people use the same Social Security number and maybe it is time for a public innovation. I would have to confess that four individuals are using my Social Security number. We have a great dane and a cocker spaniel and a stray who came to live with us, and at our vet they are all identified by my Social Security number. So if I were you, I would go back to your office and give that some exercise. [Laughter.]

In any case, thank you, very much, for your testimony.

Ms. KING. I don't know why I am surprised, Mr. Chairman. Thank you.

Chairman JACOBS. Thank you.

Now, our first panel, Mr. Joseph Eaton, author, and Mr. Robert Ellis Smith, publisher and editor of the Privacy Journal.

I am afraid that we will have to follow the 5-minute rule now on the testimony, again, in deference to witnesses who are to follow.

So, I guess Mr. Eaton is first.

STATEMENT OF JOSEPH W. EATON, PITTSBURGH, PA., AUTHOR, CARD CARRYING AMERICANS: PRIVACY, SECURITY AND THE NATIONAL ID CARD DEBATE

Mr. EATON. We should be very grateful that our Department of Defense is not taking the position that was just taken by Ms. King for the Social Security Administration. Namely, let's not use the most modern and up-dated technology to make our function more efficient. We have heard so much about the frequent misuse of the Social Security number that the disinterest in fully updating the technology that would minimize fraud is hard to understand.

Obviously, modernization couldn't be done overnight. The change of the present cards into biometric cards must be gradual in which the number and the name are verified by biometric information. Verification could be via a machine reader like we use in credit cards, easily available everywhere. This improvement would not violate privacy. It would do exactly what we are now doing.

It would enable employers, banks, or others to verify a card by just using one of those machines, and checking its biometric, preferably fingerprint information.

In the few minutes I have I would like to discuss the fact that this proposed procedure would not only greatly reduce much of the present Social Security fraud; it would enhance America's power to protect our privacy. I will not talk now about using this feature for immigration regulation or for employment verification. I want to talk about the utility of this approach for privacy protection.

If an employer asks for information with a biometric card of whether a person has a particular number, the Social Security Administration could ask that employer to verify this fact himself and verify that the employee really is the person that he says he is. As an added protection, Congress could require that any time a Government agency or somebody else accesses a personal file, the person who makes the request needs to register his biometric indicators. A trace would be left. It would require my bank, when accessing information about my credit or my mortgage to leave a trace, even though they sent in a signed permission form from me. In other words, using biometric indicators will give us the power to quickly check who is accessing any personal file, and not just in the Social Security system. It would also enable us to check what is in any one of our personal files by proving our identity.

All I would have to do is to write a letter to the Social Security Administration. After a few months—it takes them quite a while; they have a lot of files—they could send me information of what I have earned.

Under the present system, Mr. Jacobs, you or anyone else could ask for my data by giving my number and name. With a biometric indicator on my card and on your card, the Social Security Administration could say, come to the office and verify your card with your own fingerprint. Only then can we send you the information.

To sum up, because I don't want to exceed my time, the issue before us is how can we maximize the power of individuals to protect the privacy of information in this computer age where so much information is being assembled often with our cooperation, that we can't always remember what we told them.

[The prepared statement follows:]

Privacy Enhancemen Through a Biometric National Identifyer*

Invited Testimony By Professor Joseph W. Eaton

Graduate School of Public and International Affairs
University of Pittsburgh
Pittsburgh, PA 15260
Phone: 412 - 624 - 5759

Subcommittee On Social Security
Committee of Ways and Means
U.S. House of Representatives
Andy Jacobs, Jr. (D., Indiana), Chairman

Hearing on "Social Security Number As A National Identifyer"

Wednesday, February 27, 1991, 10 AM
Room B - 318, Rayburn House Office Building
Washington, D.C. 20515

America's De Facto But Imperfect Identifyer

The nine digit Social Security Number has become America's de facto national identifyer. This had not been its purpose when Congress first established this information system in 1935. The Social Security Number attained this expanded function because Congress authorized the use of this number for many other purposes, to administer the tax system, the U.S. Armed Forces, Medicare, Meadicaid and the administration of public welfare and other benefit programs. Private health insurance companies, universities, banks and many other businesses also organized their customer records on the basis of Social Security numbers. Its use has a number of administrative advantages:

a. Each person is assigned a unique number by the Social Security Administration, including children after the age of two. The number will not change, even if the person changes her name after marriage or with court approval. Even after death, the number will not be re-assigned to someone else.

b. The number provides a unique index to a person's identity but reveals no privacy sensitive information, such as race, education, profession or place of residence.

c. The number is convenient for keeping computerized records of large numbers of individuals by different Government programs, businesses and social organizations. Many have the same first or last name, but each person has a unique nine digit code,

d. The Social Security number facilitates routine matching of different data files, although almost the same degree of efficiency in data base matching can be achieved when the name and birthdat are used.

---

* Many of the ideas of this presentation are elaborated in the book by Joseph W. Eaton, Card Carrying Americans: Privacy, Security and the National ID Card Debate, Rowman and Littlefield Publishers, 4720 Boston Way, Lanham, Maryland 20706. Phone 301 - 459 3366

Unfortunately, this ID number is packaged poorly. The use of stolen and forged social security identifyers is widespread and facilitates the commission of crimes, a great deal of tax evasion and money laundering of illegal earnings.

The technology exists to issue biometrically coded social security cards that are nearly counterfeit proof. Biometrically coded Social Security cards would expose anyone using a stolen or counterfeit card to a high risk of being discovered. But there is political opposition to the adoption of this technology. The Social Security number is being used to reveal privacy-sensitive information by matching files which were assembled for different purposes.

A credit card payment for a hotel room can be used by a private investigator to collect evidence to support a charge of adultry in a divorce case by proving that a man and a woman were registered who were not married. While credit cards have their own numbering system, applicants are usually required to reveal their social security number as part of their credit application.

Members of Congress and the U.S. public is well aware that the theft or counterfeitting of Social Security numbers facilitate the commission of many preventable crimes. But enough of them are even more worried about the often semi-secret, though usually authorized used of social security numbers to engage in data base matching that individuals regard as objectionable invasion of their personal privacy.

This creates a policy dilemma. Crime fighters want to minimize the use of stolen and forged Social Security numbers in the commission of crimes, tax-evasion and money laundering that results in annual losses that exceed the cost of Operation "Desert Shield" in the Gulf War. Privacy defenders oppose anything that could contribute to the expanded use of this number by governmental or business agencies.

Both problems need to be addressed simultaneously. If American want to put a stop of maintaining what may be the least trustworthy identification system in the world the public needs to be assured that the technological improvement of the Social Security Card is balanced by the use of the same advanced technology to enhance the protection of privacy rights.

What's Needed: A Biometric Machine Readable ID Card

The twin goals of privacy enhancement and theft - counterfeit minimization can best be achieved by encouraging the use of biometric features in the Social Security Card as well as in other widely used American ID documents, such as drivers licenses, birth certificates and others.

Political controversy about this proposed modernization of documents widely used as personal ID cards can be minimized by making the reliance on biometric technology voluntary. Most persons who at the beginning will prefer to keep their present easily stolen and misused Social Security card are likely to become convinced by evidence they can observe that a biometric version would be more useful to them and more protective of their privacy. This is almost certain to happen, provided Congress balances the authorization of biometric indicators with new privacy protective legislation that relies the same tamper-resistant biometric technology.

The Case for TRIP - a Tamper Resistant Indentification Program

The updated basic Security Security card could retain the same limited personal information as the current version -- the person's name and a unique nine digit number. But it could be made almost counterfeit-proof by adding machine readable digital characteristics of the person's fingerprint. These characteristics are unique for every person.

The risk that such cards would be stolen or counterfeitted will be minimized because on important occasions, Governmental or private uses of the Social Security number could verify the ID document against the actual finger-prints of the person who presents a card as his own. Such occasions might include the following:

a. Employer verification of the person's social security number for crediting withholding taxes to their account.

b. Verification is a social security number is used as an ID document to obtain a driver's license or some other important privilege, such as a credit card, access to a classified data bank with military security implications, the right to obtain a license to practice medine. In this verification process, no personal data about the individual would be revealed. What would be confirmed is that the persons who is given the particular privilege is using his own and not someone else's identity.

Drunk drivers, who now continue driving with a second license after having their original license suspended would face the risk of being discovered. The police could check with a nationwide clearing house of Departments of Transportation if a convicted drunk driver has more than one driver's license.

Money laudering of earnings from the sale of narcotic drugs could be reduced by requiring the use of a biometric ID card for all deposits and withdrawals of large sums of money, such $ 10 000 or above.

Biometric ID cards might also be required when anyone sells jewelry, gold or other valuable to a pawn-shop, so that stolen goods can be tracked more easily than is currently possible.

Machine readers would be used when a person uses in ID card to apply for a copy of his birth certificate, a major financial benefit, such as Medicare , to claim a piece of registered mail at the post-office or when people ask a notary public to certify their signature on an important document.

We therefore have a stake that our personal personal files be administered restrictively. Access should be limited to persons with a clearly established "need to know" relationship. But it is difficult and time consuming to check to what extent these restrictions are honored.

suspected criminal act.

Persons who chose to object the inclusion of their biometric equivalents of their fingerprint in the Social Security or other ID cards would experience the inconvenience of being asked to provide other evidence of their identity, which is now happening to most people when they want to do business in a setting where they are not well known. But why should the majority of the population be deprived of the available technological protection of their privacy?

Criminals prefer to keep the current system of identification. It allows unscrupulous persons to invade our most private documents and files with little risk. Impersonation will become much more difficult if and when the proposed TRIP card becomes available to check a person's identity before are entrusted with a PIN - Personal Identification Number to gain access to a classified computerized data bank. This proposed Social Security Card and other ID card reform could be designed to have many other desirable characteristics, such as the following:

1. Freedom of Choice To Store Additional Information

Each person would have the power to decide what information, if any, should be stored on his personal card in addition to the social security number. Most people would choose to enrich their ID card into a general identity document, that would include their photograph and a digital as well as a visual reproduction of their signature. The card would then satisfy the average merchant who wants to verify a person's identity before accepting a check in payment for merchandise. Its creditability would be greater than an ordinary credit card, which is now generally used for such purposes.

2. Cost Recovery

The cost of verifying identities and re-issueing to every person a new TRIP identification card has been estimated to range between 1.5 - 2.5 billion dollars. This cost could be recovered from fees to persons who opt to obtain this new tamper resistant Social Security document.

All low income persons, below a level designated by Congress, would be entitled to exchange their existing Social Security card for the basic TRIP version free of charge. Also stored without charge would be certain public service data which individuals may choose to include, such their readiness to be an organ donor in case of death.

This replacement process would take a number of years. According to Gwendolyn S. King, Commissioner of Social Security, there are about 250 Million active Social Security Cards in circulation. About 60% were never subjected to even a most minimal validation procedure. Not all card holder would opt for the new model.

Low income persons would be allowed to add additional data, since many would be too poor to have a drivers license or own an automobile. They are now disadvantaged because they lack a creditable ID document that includes their photograph and signature.

Most Americans would be charged a modest fee if they want to exchange their existing Social Secuirty card for the TRIP model. Additional charges would be added for elective personal data, such as a digitally generated photograph, signature, and their current address. Also included could be certain medical emergency information, such as bloodtype, allergies to common drugs, and the license number to practice a profession.

Many employers would be ready to pay to have a security code added to the cards of selected employees, whom they want to have access to classified installations and files, thus making the TRIP reform program revenue neutral or generate a surplus for the U.S. Treasury.

3. A Secure Green Card For Immigrants and Long-term Visitors

The TRIP biometric model would gradually replace the present border-crossing and green cards issued to foreign workers and immigrants. For them, the inclusion of digitalized fingerprint would be compulsory. This security precaution would add a deterrent obstacle to criminals, drug smugglers and terrorists who now can infiltrate our country with relative ease with the help of forged documents. The Federal Bureau of Investigation and Interpol now maintain fingerprint files of known criminals and terrorists Such a measure is long overdue, considering the repeated threats from Islamic extremists to export terrorism to the U.S.

At busy border crossing points it would not normally be possible to check each of these cards with a digital reading machine. But the risk that such a verification process might be made at the border would serve as a deterrent to criminals and terrorists.

No "discrimination" charge could be levied against this proposed procedure. All members of the U.S. Armed forces are now finger printed, as are most Federal civil servants and police officers and other. The FBI has the fingerprints of all former U.S. Presidents in its civilian (non-criminal) fingerprint bank. There is no reason why immigrants should not be subject to this precaution which might discourage known criminals and other undesirables to enter the country and become citizens under a false identity.

4. A Privacy Neutral Central File

The identification function of the social security number can be separated from the operation of the Social Security Administration, which stores information about each person's life-time earnings and their place of employment.

The central file would contain the information submitted by the applicant , such as a birth certificate or a a school attendance record, against which a Social Security Number was assigned. It would include the person's name and any name changes that might have been requested because of marriage or a court order. The central file could be physically removed from the Social Security Administration headquarters in Baltimore, in an area of high unemployment, such as an Indian reservation.

A Social Security number entitlement would rarely have to verified against this central file. It would be used to make sure that no person could assume the identity of someone else, who has different fingerprint digital equivalents. It also would minimize the risk that someone could have more than one Social Security number.

In ordinary use, the card would be self-verifying. As George S. Warfel, Sr. suggests would be produced on carefully controlled stock, like dollar bills, with a variety of machine readable chemical security features and fine line engravings or a hologram. It would only show the social security number and the person's name. The digital equivalents of the finger-print would be stored on a magnetic strip for machine readability, if the card is verfied against the actual thumbprint of the card owner.

The privacy neutrality of this identification method is highlighted by the fact that nowhere on the card or in the central file is there any information about skin color. The digital equivalents of the fingerprint is a set of numbers, which do not permit us to differentiate between a beauty queen and someone with facial features scarred by a burn accident. It makes no statement about religion, political affiliation, place of birth, grants no privilege and denies no options.

As previously mentioned individuals would be free to pay for expanding the potential use of their Social Security Card as an identifier more trustworthy than a credit card or driver's license. They could order a card that includes their picture, current address health related information, such as their bloodtype, in case they are injured in an accident and require emergency medical service

5. Privacy Protection Through File Monitoring

Most personal files are assembled with the cooperation of the person involved, generally in return for what they believe will be a benefit. This is true of credit card applications, school records, a marriage certificate or a job application for a Federal job. What needs to be made clear through Federal legislation is that these files be viewed as the common property of the person who supplied the original information and the agency which solicited it for its administrative convenience.

Exception to this rule would be national security, FBI and police files of persons under investigation, which also would be empowered to delete information that might lead to the identification of informants.

By making explicit the proprietary right of an individual to most of his or her files, people would acquire a right of prior notice before their name or information in their file is sold for someone else's profit to a mailing list company. It would no longer be possible for mail order firms to sell a list of their customers who spend more than $ 1000 a year to a brokerage house advertising their investment service, except when the customer gives explicit permisssion in writing.

The volume of unsolicited junk mail and environmental pollution through excess waste-paper would be significantly reduced.

File owners already enjoy the right to inspect their credit reports, academic records and many others. They can check them for accuracy or to update the information.

Congress could pass legislation requiring that files designated as "privacy sensitive" can be accessed only by authorized personnel who use their TRIP card to identify themselves. This would create a record of when and by whom private sensitive information was utilized. People would be able to check periodically who was making use of their personal files and object, if among them are unauthorized users. This "leaving a trace" requirement could be extended to include the police, the FBI and the Internal Revenue Service, except in cases affecting national security and the investigation of crimes, on the basis of a court order.

Files in computerized data banks could be programmed to reject access efforts except those with authorized digital equivalents of their fingerprints. Computer hackers could no longer invade such files, as they now can by guessing or stealing the PIN access code. Nor could data base matching occur, without disclosure.

6. Privacy Ombudsman

Congress could appoint a Privacy Ombudsman, responsible for investigating allegations that private information has been improperly released or that files are being maintained in a careless manner. The Ombudsman could issue "cease and desist" orders.

Routine matching of data files would need to be disclosed to the person before he supplies the information. For instance, anyone filling out an insurance form needs to be told if the information will be checked against a national clearance file in which insurance companies exchange information to check on the consistency of information provided by each applicant.

Under the present primitive ID system, it is generally difficult to prove unauthorized disclosures or data-base matching. They have become commonplace. Many commercial firms buy lists of customers and then sell these lists to mail-order houses, political organizations and others.

Congress could also legislate fines and allow violators to be sued for punitive damages should they release data designated as privacy sensitive without authorization for monetary gain or for malicious purposes. This law could also be used to protect confidential business files against invasion by competitors - "industrial espionage". The TRIP ID card would facilitate the early detection of such offenses and thus contribute to reducing their incidence.

7. Improved Crime Control

The United States is near the top of nations in the high incidence of crime and prevalence of persons who misrepresent their identity for unlawful purposes. Their "privacy right" could be very much reduced.

Congress has already authorized Courts to search for missing parents required to make child support payments. The Social Security System is currently mandated to cooperate by locating these people whenever a social security tax payment is received that is credit to their account. Money laundering would also be made more difficult, if banks would be required to check the TRIP ID card when an account s opened. The identity of the account owner or those authorized to deposit and withdraw money would be made a matter of record.

The TRIP Card could also be coded to serve as a license to purchase, sell, transport or otherwise have access to controlled substances like poisons, addictive drugs, explosives or other designated substances that could be used in terrorist acts. Such persons could be required by law to register their machine readable characteristics as identifiers to minimize the chances that an unauthorized persons can get access to them. In case a burglary or other crime is suspected, it will become much easier to trace the person who was involved in the transaction. Persons who opted against using the fingerprint on their Social Security Card will be subjected to a more thorough screening of their identification.

8. Licensing

Organizations which maintain privacy sensitive data data files could be required to register and submit a set of privacy protection standards, including the bonding of key personnel. Most social service agencies, universities, mortgage lenders and hospitals would fall in this category.

The authority to issue a Social Security Card is currently reserved to the Social Security Administration. It lacks the staff, at present, to verify and administer the proposed more complex TRIP ID Card. Before a new card is issued, it would be necessary to check each person's credential with care, such birth certificates, passports and others. A fingerprint and a digitally readable signature would have to be taken in most cases. This process would require special technical equipment and trained personnel.

The responsibility for issuing such cards might be delegated to State offices of Vital Statistics, carefully supervised to insured the maintenance of quality standards. In addition, a system of monitoring would be required to minimize the risk that the system could be compromised by bribery or for espionage purposes. The proposed TRIP ID card would become more trusted by the general public than any of our present ID documents. Bottle necks in getting them issued would be minimized. Each State could maintain its own service, financed from a large part of the fee charged by the Federal Government from all users, except those who warrant a fee exemption because of their substandard income.

9. Pivacy Enhancement Potentialities

The benefits of living near the turn of the twenty-first century have forced us into a number of contracts with devils. We expose ourselves to sudden injury and death by traveling in fast automobiles on crowded highways. But no one would advocate that we ban this rapid transportation technology. Instead we legislate safety standards and require drivers to carry insurance.

We should apply the same principle to the up-dating of our ID card technology, There are reasons for concern that very detailed profiles could be generated by the incredible capacity of computers to store and retrieve information, derived from different files kept on each of us. An Orwellian " Big Brother" Government or business could acquire powers to harass and control.

The best defense against this "Big Brother" danger would be to use the same advanced technology to protect us against computer crimes and invasions of privacy. As much as fifteen years ago the costly victimization of American by forgers and identity thieves was described in detail in the FACFI report The Criminal Use of False Identification, issued by the Federal Advisory Committee on False Identification. But until now, Congress and the Executive Branch of Government have been willing to ignore the ease with which others can intrude into our private life on the basis of false identity documents.

Since then, our technological capacity to minimize document alterations, counterfeitting and imposture has grown impressively. It is also easier to detect and protect privacy violations, especially in files that are computerized. This also applies to misuse of confidential information.

For instance, there were 4.3 million civilians and military personnel with Federal security clearance in March 1985. Existing procedures to minimize leaks could be greatly enhanced by requiring the use of TRIP ID cards to indicate when these files were accessed. This precaution will make it easy to connect each confidential file to the persons with a "need to know" clearance.

Government building and American bases around the world can be entered during rush hours with only perfunctory clearance. TRIP cards, which are machine readable could be be verified within seconds against a physical characteristic of the person using the card.

This simple procedure would generate an automatic list of persons who were authorized to access the facility. The same could be done to produce lists of passengers on a plane. Such precautions would take little time and produce no inconvenience to the public, But they would greatly discourage potential terrorists who use false credentials.

Conclusion

Unlike Sweden, France, Germany, the Soviet Union and other European nations, the United States has managed to function without a national identification system. Thoughtful Public Service lobbyists, like those associated with the American Civil Liberties Union, the editors of the Privacy Journal and of the Privacy Times, ask the question: "Why change now?" America's democratic way of life continues to be a model for much of the world.

The "halo" of this "details of my identity are nobody's business" model has become badly tarnished. Criminals exert an inordinate influence in our social system. Privacy violations are commonplace, more often on the part of business interests than the Government. Most people have given up to limit them. It is simply too much trouble to get one's name deleted from the innumerable mailing lists that send us junk mail or automatic telephone solicitations that ring just as we sit down for dinner.

Mailing list users could be required by law to maintain an automatic service through which people could require to have their name deleted through a machine reader. They would use their TRIP ID card to transmits the digital equivalents of their fingerprint to prove that they want their name removed. The system would be close to error proof, when both the card and actual finger are used to verify each other.

The proposed TRIP ID card would provide us with a tool to monitor and counteract many of the excesses of existing surveillance technology and the computer capacity to store large volumes of information, It would become impossible to clandestinely search and combine some of our many privacy-sensitive files, like those generated by credit card companies, educational institution, medical agencies, financial institution and Government agencies.

The proposed voluntary nature of increasing the information now digitally stored for each person within the Social Security system would avoids creating a new category of dissidents or law violators. The system will become nationwide only if in the market place of ideas, a growing majority of the citizenry become convinced by the the proposed ID card reform opt to use this technology and are willing to pay for it.

Persons without a TRIP ID card will be disadvantaged in some of their business activities, much the same as those unwilling to provide their social security number or driver's license by persons who make such a request, even though they are not legally entitled to do so. They will be asked to pay cash rather than being able to pay by check.

Persons who want to serve in position of special trust and responsibility do not now have the choice to avoid being finger-printed and are required to carry special identity cards. FBI agents and Gas Meter readers are now required to present an ID card which includes their picture and their name. Their TRIP ID card would not have to reveal any additional information. The digital equivalents of their fingerprint would be invisible, but machine readable should there be a reason to subject them to this additional verification procedure.

No ID card system will be fool-proof against an occasional counter-fitting, misuse or privacy violation. But for every single case that might be dreamed up by computer hackers, there are probably thousands of criminal victimizations that will be prevented. It will also become much more difficult and risky for persons with access to privacy sensitive information, which was provided when buying a house, to sell some of it without our consent to a commercial mailing list, to private investigators or to purveyors of gossip.

Americans have a right to expect that Congress at long last assume responsibility for reforming our outdated and scandalously inefficient national identification system. It can be done within a framework that will enhance the power of each person to protect data they regard as private.

There simply is no other way to reduce the rapidly growing incidence of false identification and computer crimes. The adoption of TRIP, the biometric Tamper Resistant Identification Program would be no threat to anyone or anything, but the underworld, terrorists and to privacy violation profiteers.

Chairman JACOBS. Thank you, Dr. Eaton.
Mr. Smith.

STATEMENT OF ROBERT ELLIS SMITH, PUBLISHER AND EDITOR, THE PRIVACY JOURNAL

Mr. SMITH. Thank you.

The so-called need for a national identifier I think stems from bureaucratic imperatives. And when you weigh the convenience of bureaucracies versus the inherent right of Americans for autonomy, I think the choice should be clear.

The whole idea of a national identity card violates our American traditions, one that our Founding Fathers recognized as the need for solitude and reflection. You really cannot exercise these when you are accountable to your Government whenever you stray away from your house.

And the authors we most respect have cried out for more elbow room in our society. Our Supreme Court has followed that American tradition by recognizing a right to travel in the United States, although like privacy, you will not see the word "travel" in our Constitution, anywhere. The Supreme Court has said that "may be as close to the heart of the individual as the choice of what he eats, or wears or reads."

And then Associate Justice Sandra Day O'Connor wrote in 1983, "Our Constitution is designed to maximize individual freedom within a framework of ordered liberty." She was writing in a case that involved a young man who did nothing more than wander into affluent neighborhoods after dark. He was a law-abiding citizen, and was asked to produce "bona fide identification." One factor in that case was that America has nothing that could be called "bona fide identification." In addition to that, the Supreme Court did recognize that there is an inherent right in the United States to innocent behavior and not have to give "a good account of yourself."

Senator Simpson asked, how can we do anything about terrorism unless we have a national identifier? I think the answer ought to be in our experience. We have the best record of fighting terrorism of any nation in the world—a vast country with generally open and free travel throughout it, and lots of different ethnic groups and the amount of terrorism is amazingly low in this country. We have done that without any national piece of plastic.

The mandate, as I say, comes from small bureaucratic steps gradually. Senator Simpson is right—no politician has endorsed the idea of a national ID card, because I think they recognize that it does violate this American tradition. But there is a lesson in Australia that I cited in a footnote to my testimony. When the proposal was first made there, the polls showed that 20 to 30 percent of the people opposed it. Within 1 year, that had jumped to 60 percent and the proposal nearly brought down a government and the idea was shot down there.

Another instructive case is the Census in Germany which was suspended for about 5 years because of people's same objections to being itemized. I would also point out to Senator Simpson about the biometric commercial driver's license in California. Like so much else in this country, that mandate comes from Washington, not from Sacramento. The Department of Transportation, here in Washington, has its program to increase the identity of commercial truck drivers, and States are just simply following that mandate.

I included in my testimony about a dozen instances of how people involved in innocent activity have been stopped and asked "Are your papers in order?" Something that is reminiscent more of the Netherlands of Anne Frank than the United States.

I just ask you to multiply that by 1 million to see what will happen if we have an identity document in this country, even if the legislation says that it may be used for only one purpose and one purpose alone. Do we really believe that shopkeepers and banks and police officers would not expect a person to carry that card if it were available?

I also have some pragmatic concerns, simply that a national ID card will not work. There is no such thing as a tamper proof piece of identity. We should know that. It will lull us into a false sense of security thinking that anybody who possesses this piece of plastic will have valid identity.

I think the impetus originates really from laziness. A lot of bureaucracies don't know that they can keep perfectly good accounts of masses of people without any enumerator. The Medical Information Bureau in Boston is one good example. It keeps 11 to 12 million medical records on people and it does not use a Social Security number. It retrieves that information by a digital combination of one's name and one's address.

I wanted to alert the subcommittee to a couple of other directions that we may look for this threat to a national ID card, in addition, to the Social Security number. That is from increased technology involving bar codes which are being developed, a concept called personal number calling, which would be one telephone number to follow you from cradle-to-grave; and also the expansion of the zip code, which very shortly will zero in on every known address in the United States, and also, as Mr. McDermott pointed out, a national registry of DNA, genetic fingerprints, which the FBI is now encouraging the States to develop.

I conclude my testimony with some "modest proposals." Senator Simpson should know that the largest consumer and creator of false ID is the Federal Government, itself. We have met the enemy and it is us, and if the Federal Government were modest and conservative in its use of false ID, 80 percent of the problem would disappear.

I also think that we should have a national death index in this country, something that would not violate privacy, something that perhaps the Social Security Administration could administer in view of the testimony this morning.

I hope that doesn't mean that is a Social Security Administration reaction to my testimony?

Chairman JACOBS. No, it means your time is up, actually.

Mr. SMITH. Thank you, very much.

[The prepared statement follows:]

PRIVACY JOURNAL

P.O. Box 28577, Providence, R.I., 02908
401/274-7861

an independent monthly on privacy in a computer age

ROBERT ELLIS SMITH
PUBLISHER

TESTIMONY BY ROBERT ELLIS SMITH

PUBLISHER, PRIVACY JOURNAL, AND ATTORNEY

Before the Subcommittee on Social Security

Committee on Ways and Means

House of Representatives

of Use of the Social Security Number as a National Identifier

February 27, 1991

Writing 60 years ago, the French poet and critic Paul Valery noted: "Among living intellects, some spend themselves in serving the machine, others in building it, others in inventing or planning a more powerful type; a final category of intellects spend themselves in trying to escape its domination. These rebellious minds feel with a shudder that the once complete and autonomous whole that was the soul of ancient man is now becoming some inferior kind...that wishes only to collaborate, to join the crowd, to find security in being dependent..."

Valery went on to observe: "The most redoubtable machines, perhaps, are not those that revolve or run, to transport or transform matter or energy. There are other kinds, not built of copper or steel but of narrowly specialized individuals: I refer to organizations, those administrative machines constructed in imitation of the impersonal aspects of the mind."[1]

We should remember that the laureates of the presumed cybernetic nightmare -- Kafka, Orwell, Huxley -- were in fact rebelling against impersonal bureaucracies more than computerization. The anti-utopias in George Orwell's 1984, Aldous Huxley's Brave New World, and Yevgeny Zamyetin's We are bureaucratic tyrannies, not necessarily computerized tyrannies.

The "need" for a national identity document or for increased uses of Social Security numbers comes from these bureaucratic machines, which now dominate our society. When we weigh the convenience of bureaucracies against the inherent rights of Americans to autonomy and independence, the choice should be clear.

Washington Address: P.O. Box 15300, Washington, D.C., 20003

A mandatory national identity document would remove most of the flexibility from American life. Our founding fathers -- Jefferson, Adams, Madison -- spoke of the need for solitude and reflection. You can not practice these when you are accountable to your government whenever you stray from your house. From William Penn to Henry David Thoreau to Walt Whitman to Horace Greeley, our essayists have cried out for more elbow room.

America stands today as one of the very few places where citizens have the freedom to travel without internal controls -- and vast open space in which to exercise that freedom.

The right to travel in America "may be as close to the heart of the individual as the choice of what he eats, or wears, or reads," said our Supreme Court in 1958. Associate Justice Sandra Day O'Connor wrote in 1983, "Our Constitution is designed to maximize individual freedom within a framework of ordered liberty."[2]

But we all take it for granted. What has happened to the spontaneity of American life? The informality? The association with the natural environment? The freedom? Have we traded it for convenience and accountability?

Throughout our history, our most creative impulses have emerged out of risk-taking, out of chaos, out of a freedom to make mistakes. They have not been generated when we have been observed, recorded, enumerated.

Some bureaucrats insist that the country would run more smoothly if we all were compelled to carry a unique, counterfeit-proof plastic identity card. They seem to forget that a large number of Americans -- or their parents -- came to the United States to escape oppressive requirements that they always carry "your papers" with them.

In the past 60 years, the instincts of the American people have been right about the matter of mandatory enumeration. When the Social Security system was established, there were intense debates about the possibility that the Social Security number could become a de facto national identifier. (Legislators promised this would never happen.)[3] Americans at that time were aware of the abuses of Nazi Germany.

In spite of constant concerns about crime and fraud and illicit dealings, the American people are still wary of a national identity document. In an opinion survey by Louis Harris last year, 56 percent of those questioned opposed even the idea of a national work identification card to distinguish between illegal aliens and citizens or resident aliens.[4]

Older people, who remember the Nazi experience, are probably more wary of enumeration than younger people, who have grown up with plastic cards and multi-digit numbers. We should remember that the last great uprising in this country (in the 1960s) began not with the cry, "Stop the War," but a few years earlier with the chant in Berkeley: "I am a Student. Do Not Fold Bend or Mutilate."

Politicians sense this strain in the American character, and not one has endorsed the idea of a national identity document. Bureaucrats sense this opposition as well, and so, being bureaucrats, they press not for a national ID number immediately but for authority to enumerate only their own constituency, to serve their narrow needs -- without regard to the cumulative impact of these gradual intrusions on the citizenry as a whole.

"A national ID card," they say, "would be used only for employers to establish citizenship. It would not be used to cash checks. Police could not require you to produce it on the street. We'll make sure by legislation." But is it realistic to expect that such a policy would remain for long?

And so the nightmare of a national ID number is upon us, because of a series of small bureaucratic baby steps, not as the result of a deliberate national decision.

The Specter

Even without a mandatory national ID number, we already have enough horror stories to give us a glimpse of what will happen to millions of Americans. These cases actually happened:

1. An innocent black man is stopped and arrested 15 times in two years while walking in a white neighborhood, merely because he does not produce "bone fide identification."

2. A Washington woman is put off an Amtrak train in Philadelphia because she is unable to produce a driver's license, even though she paid for her ticket in cash.

3. A man jogging in Washington is detained by police because he is not carrying identification.

4. A swimmer in California is arrested for "resisting arrest" because she cannot produce a photo identification.

5. The affluent community of Palm Beach, Florida, tries to require by ordinance that non-residents employed in the town carry identity cards and produce them upon demand.

6. A parish in Louisiana tries to require "itinerant laborers" to register and carry ID cards.

7. A Native American parent is required to obtain a Social Security number for his four-year-old daughter even though this violates his sincerely held religious beliefs.

8. A Chicago woman, after making an illegal left turn, is locked up in the city jail and strip-searched because she could not locate her driver's license.

9. The water company in a New Jersey city tries to require each of its customers to identify, by Social Security numbers and relationships, anyone living in the household.

10. A Nebraska woman is compelled to spend thousands of dollars in legal fees to protect her right to have a driver's license without foregoing her sincerely held religious belief against being photographed.

11. The school system in Tulsa, Oklahoma, requires a pupil of any age to provide a Social Security number before attending classes.

12. Police officers in California demand Social Security numbers of persons arrested for traffic offenses.

13. The largest bank in the U.S., Citicorp, answers its toll-free retirement account line not with "Hello," but, "What is your Social Security number?"[5]

Is this our vision of America? Or is it closer to the wartime Netherlands of Anne Frank?

Pragmatic Concerns

A national ID card won't work. First, we know from experience that there is no such thing as a tamper-proof identity document.[6] A high-tech national ID will simply raise the ante on the street for phony IDs. And, as shopkeepers, police officers, and bureaucrats are led to believe that the new document is counterfeit-proof, they will place increasing reliance on the validity of the ID card. Our current willy-nilly non-system of identity may seem unreliable to many; but that may be its strength. At least most of us know better than to place great faith in the validity of current IDs. We should not be lulled into a false sense of security. We know, or should know, that the best assurance of identity is personal recognition -- or its surrogates.[7] Reliance on numbers deceives us into thinking we have accurately established identity.

We need only look to those institutions in American life that are most intensively enumerated now -- prisons, the military, corporate America, colleges and universities. In each of these segments, identifying -- and enumerating -- the population is not difficult. Yet these are places where crime and fraud occur at a rate higher than -- or at least as high as -- in the population as a whole.

James Q. Wilson, the law-enforcement expert at Harvard, makes the point that we know who the criminals are in each community. They keep committing the same crimes over and over again. Police departments know who they are. It's not as if the police need to place a number on each criminal in order to know who they are. Nor is it common that criminals use Social Security numbers or leave their true IDs at the scene of the crime.

Laziness

Organizations insist on Social Security numbers mainly out of laziness. It's a number that most people can remember. Demanding the number is a way of persuading people that they can be tracked down after any wrongdoing -- a returned check, an inflated resume, a failure to report income to tax authorities.

Yet, in the 1990s, large organizations are able to store and retrieve massive amounts of personal data without resorting to Social Security numbers or any other numbers. MIB Inc. (the Medical Information Bureau), which stores medical codes on more than 11 million insured Americans, is an example. IBM Corp., long ago abandoned SSNs as employee numbers for its thousands of personnel.

Alternative Threats

It is not news that the Social Security number has become a virtual mandatory national identity number -- even if a seriously flawed one. What is news is that there may now be alternative routes towards the much-feared national ID.

Several companies -- like United Parcel Service and Matsushita -- are experimenting with a bar code, like the black and white Uniform Product Code on groceries, that will contain letters as well as numbers. UPS wants to use its own variation of the bar code to include names, addresses, and routing information. Using similar technology, some states would like to add a bar code to drivers' licenses. A bar code could be issued to each man, woman, and child in the U.S., encoding name, address, and even personal information.

Bellcore, the research arm of AT&T, is developing a concept called PNC, Personal Number Calling. This would permit the same phone number to be used for home phone, vacation home, office, modem, auto phone, pager, and fax machine. One PNC could be issued for the duration of your life, a means to summon you anywhere.

The U.S. Postal Service has already expanded the Zip Code to nine digits, targeting a group of 200 people or fewer. Now the Postal Service is expanding the Zip Code further, so that a distinct number could be assigned to virtually every address in the U.S. Part of the USPS plan is to create a list of every known address in the U.S.

Urged on by the FBI, states are building data banks of individual genetic codes (DNA "fingerprints"), which are said to be unique with each individual. The current thinking is to require these codes only of those convicted of violent crimes. MIT sociologist Gary T. Marx asks, "Through a process of 'surveillance creep,' will this spread to those convicted of non-violent crimes? And will mandatory genetic 'fingerprinting' eventually be required of the population at large?"

While we have been worried about the Social Security number as a form of national ID, we have not realized that a national identifier may come from other sources.

Proposals

Congress, which originally promised the American people that enumeration would not go beyond Social Security record-keeping, has regularly since 1970 opened the floodgates a little to permit new uses of Social Security numbers. Private businesses have followed the lead.

It is time for Congress to do something it rarely does: reverse a trend, not merely codify it.

Congress should:

1. Prohibit the enumeration of children under the age of 16 years of age for any purpose. (There is time enough later in life for young Americans to feel the dehumanization of enumeration).

2. Limit federal, state, and local government uses of Social Security numbers to transactions that produce income or create tax-reporting requirements.

3. Require private businesses to accept only the last four digits of a person's SSN in any transaction, except where Social Security numbers are required for tax-reporting purposes. (This meets the needs of organizations that say they need the number to prevent duplications or distinguish similar names.)

4. Prohibit a private entity or government agency from displaying a person's Social Security number on any publicly available document (including mailing labels and envelopes).

5. Create a National Death Index to record the identity of persons who die, so that birth certificates, Social Security cards, and other identity documents are not reissued to persons using their names.

6. Require local registrars of vital statistics to mark a birth certificate "deceased" when it knows or has reason to know (through the National Death Index) that the subject of the birth certificate has died.

7. Prohibit government agencies from using and creating false identities except in compelling cases of life-and-death approved by the head of an agency.

It is ironic that less than one year after we Americans rejoiced in the liberation of peoples in Eastern Europe we are seriously considering adopting a means of social control that Eastern Europeans rejected soundly.

One year after we rejoiced in the liberation of a man whose movements are restricted in South Africa because his "papers are not in order," we are considering a "domestic passport" similar to that in South Africa.

At a time that we are at war with a regime that categorizes and oppresses its people, can we seriously be considering a plan that could have no other purpose in this country?

The late J. Braxton Craven Jr., of the Fourth Circuit Court of Appeals, spoke of "personhood," not "privacy," when categorizing the unenumerated Constitutional rights that make Americans special. In reference to the right of personhood, Judge Craven wrote:

> To the average person, who may not wish to make a speech or print a newspaper, it may be the greatest freedom of all. The right to be let alone is the only non-political protection for that vast array of human activities which, considered separately, may seem trivial, but together make up what most individuals think of a freedom. I am thinking of little things, mostly taken for granted, such as the right to attend a football game, to refrain from attending a political rally, to wear a hat, or to ride a bicycle to work through city traffic.

Now, will we require a plastic card to engage, or not engage, in these simple pursuits of "personhood"?

Will we do this in the name of keeping undocumented aliens from our menial jobs or in the name of preventing a few from double-dipping into our inadequate public-assistance payments?

If we do, we will lose the soul of America.

Footnotes:

1. *The Collected Works of Paul Valery* (Princeton University Press, 1962), quoted in Fairy Tales for Computers edited by Leslie George Katz (The Eakins Press, Boston, 1978).

2. *Kent v. Dulles*, 357 U.S. 116 (1958) and *Kolender v. Lawson*, 461 U.S. 367 (1983).

3. *Report on the Collection and Use of Social Security Numbers* by Robert Ellis Smith (Privacy Journal, Providence, R.I., 1991), p. 8.

4. Louis Harris & Associates National Opinion Survey (Equifax, Atlanta, 1990), p. 23. By contrast, Gallup Polls in Australia in 1986 showed only 25 to 30 percent in opposition, but this was enough to build into Parliamentary opposition that killed a proposal for an "Australia Card" and nearly brought down the Government, according to "Just Another Piece of Plastic for Your Wallet: The 'Australia Card' Scheme" by Roger Clarke, Prometheus , Vol 5, No. 1, June 1987. Within one year the percentage in opposition had jumped to 60 percent.

5. (1) *Kolender* v. Lawson, 461 U.S. 367 (1983); (2) letter to PRIVACY JOURNAL; (3) letter to PRIVACY JOURNAL; (4) letter to PRIVACY JOURNAL; (5) Wallace v. *Town of Palm Beach*, 624 F. Supp. 864 (S.D. Fla. 1985); (6) *Service Machine & Shipbuilding Corp. v. Edwards*, 617 F. 2d 70 (5th Cir. 1980); (7) Bowen v. Roy, 476 U.S. 693 (1986); (8) *War Stores* (Privacy Journal, Providence, R.I., 1990); (9) ibid.; (10) *Jensen v. Quaring*, 472 U.S. 478 (1985); (11) *Report on the Collection and Use of Social Security Numbers* (Privacy Journal), p. 22, and PRIVACY JOURNAL, December 1990, p. 5; (12) 90 *Daily Journal* D.A.R. 12664 (Nov. 9, 1990) and PRIVACY JOURNAL, December 1990, p. 7; (13) files of PRIVACY JOURNAL.

6. "The Criminal Use of False Identification," by the Federal Advisory Committee on False Identification, U.S. Department of Justice (Washington, D.C., 1976). Robert Ellis Smith served as a member of the advisory committee.

7. Ibid.

Chairman **Jacobs**. We will go to Mr. McDermott.

Mr. **McDermott**. Thank you, Mr. Chairman.

I have no questions. I concur basically with your testimony.

Mr. **Smith**. Thank you.

Chairman **Jacobs**. Mr. Gibbons.

Mr. **Gibbons**. Mr. Smith, I think your idea of a national death registry is a good idea. It is very difficult to tell when someone has died. [Laughter.]

But I am sure that many a dollar has been defrauded away from the Social Security Administration by just not being able to trace back that someone has actually died.

Mr. **Smith**. Not only that, but the main use of false ID starts with the birth certificate where people get fraudulent birth certificates after going through cemeteries and looking for somebody about their age who has died. I am told that local registrars of vital statistics oppose this proposal. It was originally thought that maybe the National Cancer Institute or something of that sort could administer this but perhaps Social Security would be the better house for this.

Mr. **Gibbons**. In these other attempts to get other identification methods, such as genetic fingerprints and things of that sort, are these designed to produce national registration systems?

Mr. **Smith**. No, not at all. The genetic fingerprints data bases would be strictly confined to the criminal justice field. They would be combinations of DNA prints taken at the scene of a crime and also those prints of people who have been incarcerated. The legislation would say that it could only be used for that purpose but my fear—and I think that Mr. McDermott alluded to it—is that through the "slippery slope" eventually it will be used for other purposes. And law abiding citizens will be expected to have their DNA prints on file; that's the fear.

Mr. **Gibbons**. Thank you.

Mr. **McDermott**. Just to followup on that, the genome program which is essentially the tracing of the DNA in human beings is progressing at a rapid rate, and our ability to identify a variety of illnesses. Once that genome program is in place, you are going to have an insurance company that will demand a drop of blood from you, from which they can decide what illnesses they will not cover, even though you only carry the gene for it, you do not have the illness.

So to me the potential for this is so widespread people really are not thinking about how it, what the access really can be in the future. It just seems to me that incrementally you get dragged into this kind of thing and you don't realize it. That's why I am very reluctant to think about a national identifying card which has biometric information on it, because I suspect that you will also shortly be able to put the DNA code right on the biometric information that is on that card. So that you will have it all with you at all times, and when you apply for a job or anything else, and put that card in and can tell whether they want to hire you because you carry the gene for diabetes or whatever.

I mean the potentials for it are enormous.

Mr. SMITH. It's a time bomb because you will be carrying around something that is machine readable and you could not read it yourself.

Chairman JACOBS. Well, the subcommittee is in the debt of the panel. We thank you, for your balanced views, and we will go on to the next panel.

Mr. Warfel, you may proceed.

STATEMENT OF GEORGE H. WARFEL, SR., CHAIRMAN, WARFEL ASSOCIATES INC.

Mr. WARFEL. Thank you.

I am George Warfel, Sr., and my company is Warfel Associates Inc., a technical consulting firm engaged solely in offering advice and consultation of biometric personal identification and plastic card technology.

Given the time limitations, I will summarize the first 2½ pages of my written testimony in 1 minute and devote the rest of the time to the biometrics which seems to be something not too well understood in this room.

I will single out fingerprints as the suggested method of identifying our citizens nationally.

Page 1 of my testimony says that I am in favor of a national identifier but one without a central data base of listed personal traits or preferences. A national identifier should be a card containing only name, serial number, and a biometric fingerprint record, thus, it could be used only by the person to whom it was issued.

Page 2 explains the design of such a card, and the first half of page 3 gives a manufacturing guidelines suggested in processing such a card.

Now, for biometrics. The bottom of page 3, there are six categories of biometrics that are shown symbolically. The first one, eye-scan, has been used for several years to control the flow of people in and out of highly secure locations. It is an excellent identifier for such a place—war rooms, drug vaults, Ft. Knox, things of that nature—but eye-scan is not well suited for an entire national population.

The second biometric on the diagram is based on hand-shape. Hand-shape is a good identifier where it is used frequently, where the identifiee frequently places his hand for identification. Incidentally, the word, frequently is omitted from the written testimony, a typo among others, on the left side, in the next to the last line of page 4. I will revise that before I submit it for printing.

I can't see hand-shape as the best biometric identifier for the general public. Voice, as an identifier, has an excellent track record. However, it is useless unless the identifiee wants to speak and is willing to speak and is able to speak a few words in a normal voice. This is not always possible in a noisy crowded site, or an emotional situation.

The fourth biometric is a learned muscle pattern, such as handwriting—the way you sign your name, walking, shaking hands, any other frequently repeated physical effort such as a golf swing that some people perfect that I have yet to achieve. Muscle dynamics are not suitable for a national identifier, however, because of the ease with which they may be altered intentionally.

Eliminating these four leaves us with facial features and fingerprints as national identifiers. Both would be excellent. The automated recognition of faces has been tested and found very good using neural computers and a small data base. The technology is in its infancy and it is very expensive, but it does work. Acceptable hardware is years away.

That leaves us with fingerprints, seems to be the winner, almost by elimination. I would suggest that a card containing a fingerprint of the proper cardholder is the national ID solution. I have in mind a card that when I grip my thumb and forefinger on the right corner at the bottom, it would identify me with perhaps a red light or a green light, something like that. But if you should use it, your fingers in that location would not cause the card to function. It would warn you that it was not your card.

Fingerprints says nothing about sex, even skin color, age, race, hair color, none of that is in a fingerprint. But the fingerprint would say that it was your card. It contains nothing, absolutely zero information on personal habits or preference. My fingerprint doesn't change if I change my religion. It doesn't change as I grow older and my hair turns white. Fingerprints have been in use for over 100 years. And unfortunately they were used primarily for criminal identification and people say, I don't want to be ID'd like a criminal.

But that is an emotional situation. We are now fingerprinting college professors, school kids, Federal employees, all kinds of people. But we do not require that the identifiee even be cooperative or even alive to give a fingerprint. They do not change throughout the life. Even if it is removed by injury, it returns in the same form. Thus, a fingerprint is, indeed, a biometric—one of many—and I suggest that we use it as a national identifier.

Thank you.

[The prepared statement follows:]

WARFEL
ASSOCIATES INC.
Since 1973

P. O. BOX 627, MENLO PARK, CA
(415) 854-4923 94026

GEORGE H. WARFEL, SR.
CHAIRMAN

Statement and Outline for Congressional

Hearing, 2/27/91

(Subcommittee on Social Security)

A NATIONAL IDENTIFIER --A CARD WITH NO DATABASE

Our American system of democracy tolerates more individual freedom than any civilized country in the world. There may be some undeveloped countries, without central governments, where more freedom (and near anarchy) exists. But our American life is the envy of every freedom loving person on earth. We must thank God, the founding fathers and the subsequent generations of dedicated lawmakers, that we still enjoy that freedom.

As the population grows and our cities become more crowded, our individual freedom is eroding dangerously. The single factor that bears the greatest responsability for that diminishing freedom, is that we allow our criminal and near-criminal activists to hide under false names and fake identity.

They are not the leaders; leaders have to be well known to succeed. They are the noisy front rank followers. They are the ones drawing welfare under multiple names. They pay minimal taxes on large undeclared earnings. They are the gangs that make our streets unsafe. They are the thieves that rob our homes. Many of them are not even citizens, or legal aliens.

When they are apprehended by law enforcement agencies, they have no record - under the name they are using at the time. So, they are set free to go on to the street under still another new name.

If we are to keep these people from ruining our democracy, we must limit them (and ourselves) to one identity. It will not hurt us, we can continue our life in our present fashion. But it will stop the underworld operators the first time they break the law.

I do not suggest a dossier or a data base on everyone. Existing information files must stand or fall on their own merits. I merely ask that we all be allowed only one name, one identity, and that it be documented by a card. We can keep the card in our wallet. There need be no central file except that required to assure that one and only one card exists for each person named. The central file would say nothing about age, sex, religion, race or any other personal detail. It would contain only name, number and date of issue.

The card would assure:

o That the existing files were not erroneously related to the wrong person.

o That no person could assume the identity of another.

o For a person to have more than one identity would be impossible.

o No person could have the benefits of our society without maintaining an identity.

o That a personal file could be accessed only after the accessor was clearly identified and had proved that permission had been granted by the subject file person.

SIX STEPS IN DESIGNING A SECURE CARD

1. The basic material (probably paper or PVC plastic), called "stock", must be such that it is recognizably unique by sight, feel or both.* The stock must not be used for any other purpose.

Example: The paper used in dollar bills.

2. The process of creating a blank card from this stock must also leave a condition or feature that is recognizably unique by sight, feel or both.*

Example: The fine lines of the engraving on blank securities certificates.

*Note: The unique qualities in the material, and the conditioning when the blank is made, must be readily machine detectable.

3. Each blank card must be marked with a number such that there are no two alike. These numbers must be machine readable and not of a standard set (such as OCR-A or B, or E-13B). The font must be copywrited and restricted from any other use.

Example: Plastic credit cards.(Except for standardized 7B font.)

4. The blank card must then be personalized by assigning it a persons name and perhaps a picture or signature. The digital data should be in the same font as in 3, above.

Example: The typical state issued driver license. (Except for font similarity.)

5. A biometric feature** of the individual involved in step 4 must be applied. This need only be machine readable.

Example: The INS border crossing card of the 1980's.

6. There must be a final processing that will clearly signal any attempt to alter the data on the card. The indication of alteration must be machine readable as well as visible.

Example: Cards protected by die release film or optical distortion film.

** The suggested biometric would be the fingerprint. The fingerprint record of the true cardholder would be in the card, NOT in a central file. Thus the card could be used only by the person to whom it was issued.

A fingerprint:

Does not reveal the subjects skin color.

Does not reveal sex or sexual attitude.

Provides no record of age or hair color.

Makes no statement about religion.

Says nothing about political affiliation.

Is the same regardless of race, nationality or ethnicity.

Grants no privilege.

Denies no options.

MANUFACTURING GUIDLINES FOR SECURE CARDS

Each of the above six procedures must be done according to the following guidelines:

O The processing machines must be so large that no one of them can be hidden in the trunk of a car or in the average clothes closet.

O The machines must be so heavy that three men are required to move any one of them.

O Each step must require the skills of three or four persons.

O Workers should not be cross trained in each others jobs.

O The machines involved must not fit any other use or purpose.

O The site of the card processing equipment and all associated storage facilities must be open to view but protected by glass on all sides.

WHY?

These guidelines are to make it nearly impossible for one man working alone, in small secret quarters, to succeed in creating a counterfeit card.

If the machines are large and not usable for any other purpose, they will likely be seen by a house cleaner or delivery person and reported to police. If they are too big to hide, the police will find them. If they cannot be used except to make cards, the owner would be unable to explain their presence falsely.

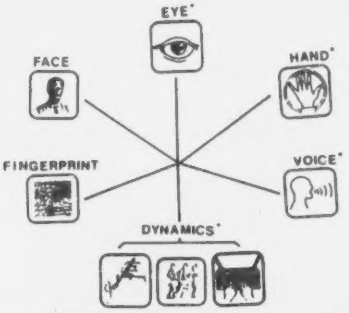
The need for three or four persons to be involved in setting up, moving and operating the machines, is to increase the likelihood of someone reporting (squealing) on any improper operation.

BIOMETRICS - - A FRAUD-PROOF IDENTIFIER

A biometric is defined as:

> ".....a measurable physical characteristic or personal trait used to recognize the identity, or verify the claimed identity, of a person through automated means." (International Biometric Association, founded in 1986 under the guidance of Warfel & Miller, Inc.)

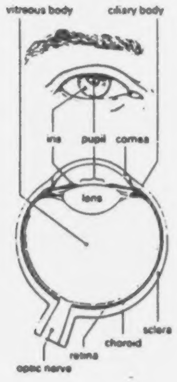
It is generally recognized that there are six categories of biometric traits, plus the new DNA. The six are symbolically shown below.

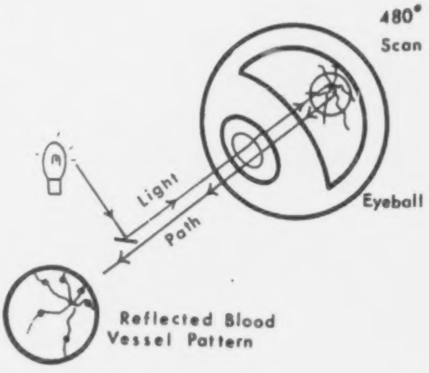


Not all biometrics are suited to public ID. For example, the method must be usable on a person who is uncooperative (perhaps from substance abuse) or unconscious, or dead (from an accident). The method should not be invasive as in blood testing, or undignified as urine testing. The biometric should be unchangeable (even by surgery) for life.

Let us look briefly at the biometrics.

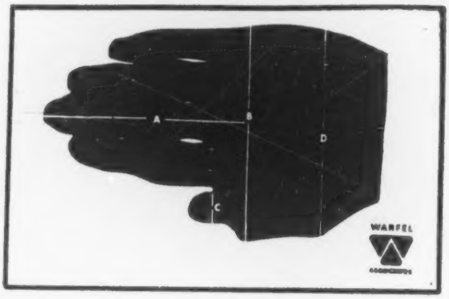
EYE SCAN: The rear wall (the retina) of the eyeball has a blood vessel pattern that is different in every individual. There are machines that will scan this biometric and can thus identify a person. It does require the cooperation of the individual because the iris lens must be focused into the machine. A person can avoid identification intentionally by not focusing. Also a dead or unconscious person cannot use this method for identification.





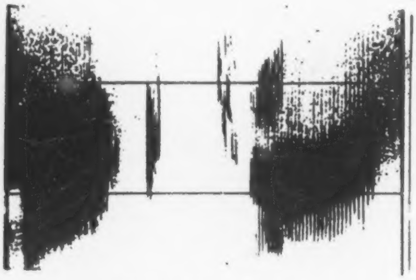
HAND SHAPE: The hand shape method is best suited to cases where it is used. Again the identifyee (person being identified)must be willing and helpful. The hand shape is in use many places as an employee ID.

VERTICAL HAND PROFILE



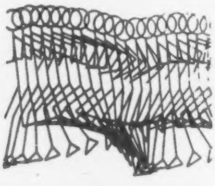
VOICE: We all use voice to identify our friends in everyday relationships. The are machines that can recognize voices with a high degree of accuracy. As in the two above, however, the identifyee must cooperate. If the subject remains silent, as is a persons right, it is not possible to make an ID by voice.

Employee Identifying Himself
By Voice At Room Entry.

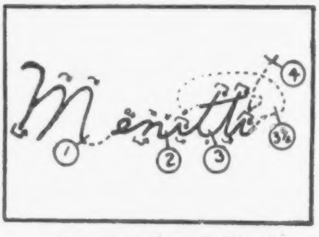


"Voice Gram" Of A Person

MUSCLE DYNAMICS: There are many things we have learned to do by habit and we will always do them the same way - if we want to. A golf swing is always the same, when done by a pro (and some good amateurs, not including myself). The way one walks, is a learned habit and remains much the same during middle life. The dynamic motion of a signature is an excellent way to identify a true signer from a forger. Banks are using it today where large sums are involved. The dynamic methods have the same drawback as the voice. If the identiftee refuses to sign, or changes his scrawl deliberately, it is impossible to make an ID.



Stride or Gait is a
Biometric Identifier



The Speed and Rhythm of a
Signature Can Tell the True Signer
From a Forger

FACIAL FEATURES: The face is something that remains as the single most used identifier. Not only in personal social situations, but there are now machines that can identify video images with a very high degree of accuracy. Cost is the drawback to this method. With further research the cost will come down, but the day of "off the shelf" image recognizers is at least ten years away.

176 *Identification Technologies*

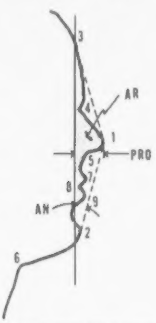
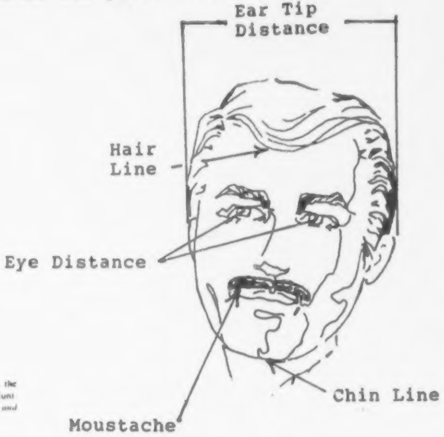


Figure 31. The profile, though seldom used in manual recognition, is the best suited to machine analysis. (From L. D. Harmon and W. F. Hunt, Automatic Recognition of Human Face Profiles, *Computer Graphics and Image Processing*, 1977. Courtesy of Academic Press, New York.)



FINGERPRINTS: Fingerprints were originally used (in the late 1800's) to identify criminals. Today we are fingerprinting bank employees, college professors, civil service employees, drivers (upon application for a license) and even school children. Finger prints do not change throughout life. They can be used to identify the dead even years after death. No two people have ever been known to have identical prints. Machines have been developed that can read and analyze fingerprints in seconds; minutes in difficult cases.

CONCLUSION: Of all of the biometrics, fingerprints seem the most suited to a national identifier. I would suggest that the prints be stored in a card carried by the subject; NOT stored in a central data base. The technology to do this has been researched and patented. It needs to be funded for engineering and made into a product, but it is possible.

Chairman JACOBS. Thank you, Mr. Warfel.
Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, DIRECTOR, WASHINGTON OFFICE, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY

Mr. ROTENBERG. Thank you, Mr. Chairman.

My name is Marc Rotenberg, and I am the director of the Washington office of Computer Professionals for Social Responsibility. I am going to speak generally about the use of the Social Security number and the problems in using this number for purposes unrelated to that which it was originally intended.

I would like to say that briefly that I agree with many of the comments that Mr. Warfel just made regarding high-end identification technologies, but I would caution that the application of these technologies should generally be limited to special purposes—military installations, secure sites.

The concern with the use of a Social Security number is quite a bit more far-reaching and I would like to give, by way of illustration, some work that our organization did during the past year, almost since the time that Congressman Bob Wise held a hearing on the creation of a data protection agency last year which we testified at.

We told Mr. Wise about a product called Lotus Market Place that contained a great deal of personal information about American consumers had not been released. We cautioned that there were serious privacy problems with this product and during the subsequent months were able to uncover the fact that the information in the Market Place product was keyed to the Social Security number. When we learned this, we formally opposed the release of the product, and Lotus and Equifax, the two companies that had developed it, announced just in the past month that they would, in fact, not sell this product.

I want to say, at this point, that the congressional record of stringent restrictions on the use of Social Security numbers is quite strong, even though you will hear witnesses testify to the expanding use of the Social Security number. By way of illustration I would mention a few conclusions that were reached in a landmark Government report in 1973 called, Records, Computers, and the Rights of Citizens.

Regarding the use of the Social Security number, the report concluded first, that the use of the Social Security number should be limited only to those purposes required by the Federal Government; second, Federal agencies should not require the use of the Social Security number, absent statutory authority; third, Congress should evaluate any proposed new use of the Social Security number; and then that individuals should have the right to refuse to provide their Social Security numbers and should suffer no harm as a result of exercising that right.

Now, these principles, recommended in 1973, are very strong and if you read the report you will find, in fact, that the committee members do not mince words. The following year, 1974, Congress passed the landmark Privacy Act. Congress was equally clear in this law about the stringent regulation that must be applied to the Social Security number. This is what the Privacy Act said: It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his or her Social Security number. It went on to say that any Federal, State or local government agency which requests an individual to disclose his or her Social Security number shall inform that individual whether the disclosure is mandatory or voluntary, by what statutory authority the number is solicited, and what use will be made of the number. That is in the Privacy Act of 1974. It is a very strong statement designed to restrict the use of the Social Security number.

Now, we think that this is a basis upon which further congressional activity could begin, and in particular, we are most concerned about the growing use of the Social Security number in the private sector. We do not think that it is necessary for organizations that maintain large file systems to use the Social Security number to efficiently maintain their system of records. As Bob Smith described just a moment ago, there are very large record systems that find other methods for creating an index key that both works from the organization's viewpoint and protects the privacy rights of the individuals.

Therefore, we would urge the committee to consider legislation that would prohibit private organizations from requesting the Social Security number absent explicit statutory authority. Where the law requires the business to collect the Social Security number, they should be allowed to do so. Absent such authority, we would like to prohibit the use of the Social Security number.

Thank you.

[The prepared statement follows:]

TESTIMONY OF MARC ROTENBERG
COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today on the use of the Social Security Number as a national identifier. My name is Marc Rotenberg and I am the director of the Washington Office of Computer Professionals for Social Responsibility.

CPSR is a national membership organization of computer scientists from across the county. Our membership includes a Nobel laureate and four winners of the Turing Award, the highest honor in computer science. CPSR has a particular interest in privacy issues, and we have testified before several Congressional committees in support of efforts to protect privacy.[1] We are pleased to be here today, and thank you for convening this hearing.

I will this morning describe the privacy problems with the current use of the Social Security Number particularly in the private sector. I will then recommend that Congress take strong steps to curtail the misuse of the Social Security Number. First, I would like to describe for the Committee a recently cancelled product that CPSR opposed in part because of the misuse of the Social Security Number. This brief discussion of the product, Lotus Marketplace, should help to illustrate the problems with the misuse of the Social Security Number in the privacy sector.

---

[1] See "Computer Privacy and the Need for the Establishment of a Data Protection Board," the Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations, U.S. House of Representatives, May 16, 1990; "Computer Virus Legislation," the Subcommittee on Criminal Justice, Committee on the Judiciary, House of Representatives, November 8, 1989 reprinted in Computer Virus Legislation, 101st Cong., 1st Sess. 25 (1989); "The Redesign of the National Crime Information Center (NCIC)," the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, House of Representatives, May 18, 1989 reprinted in FBI Oversight and Authorization Request for Fiscal Year 1990, 101st Cong., 1st Sess. 512 (1989); "The Computer Security Act of 1987 (P.L. 100-235) and the Memorandum of Understanding Between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA)," the Subcommittee on Legislation and National Security, Committee on Government Operations, House of Representatives, May 4, 1989 reprinted in Military and Security Control of Computer Security Issues, 101st Cong., 1st Sess. 80 (1989); "Amendments to the Fair Credit Reporting Act, before the Subcommittee on Consumer Affairs and Coinage of the Committee on Banking, Finance and Urban Affairs, House of Representatives, June 12, 1990, reprinted in Amendments to the Fair Credit Reporting Act, 101st Cong., 2d Sess. 774 (1990). See also "In the Matter of the Application of the Chesapeake and Potomac Telephone Company to Offer Caller ID with Special Identification Arrangements," Public Service Commission of Maryland, Case No. 211, August 31, 1990; "In the Matter of the Application of the Chesapeake and Potomac Telephone Company to Offer Return Call and Caller ID within the District of Columbia," Public Service Commission of District of Columbia, Formal Case No. 891, March 22, 1990.

LOTUS MARKETPLACE AND THE SOCIAL SECURITY NUMBER

Mr. Chairman, last May CPSR testified before Representative Bob Wise's Government Information Subcommittee in support of new privacy legislation. We recommended that the United States establish a data protection agency to promote the development of new privacy laws and to act as a privacy ombudsman. We said that this proposal was the missing piece in U.S. privacy law.

In response to Mr. Wise's inquiry about new privacy problems in the private sector, we raised concern about a then unreleased product called Marketplace. As described in promotional materials, this product was to contain personal information on 120 million American consumers, including name, age, address, estimated annual income, marital status, and gender, as well as modelled data that revealed buying propensity.

We advised Mr. Wise that the Marketplace product would violate conventional standards of privacy protection, as defined by both the computing profession and generally accepted standards for records management.[2] We also raised particular concern about the burden that would be placed on consumers who wished to exercise the "opt-out" option and ensure that their information would not be included in the product.

During the months that followed Mr. Wise's hearing we continued our assessment of Marketplace. Following inquiries by several of our members, we determined that the underlying data provided by the Equifax Corporation to the Lotus Corporation was keyed to the Social Security Number. That is to say that each individual's record contained in the Marketplace data base was indexed on the Social Security Number.

We learned this when individuals who did not want their personal information included in Marketplace contacted Equifax and were told to fill out a form indicating not only their name and address but also their Social Security Number.

---

[2] The Association for Computing Machinery (ACM) Code of Professional Conduct states that:

> An ACM member should consider the health, privacy and general welfare of the public in the performance of the member's work. (E.C. 5.1)
>
> An ACM member, whenever dealing with data concerning individuals, shall always consider the principles of individual privacy and seek the following: To minimize the data collected; To limit authorized access to the data; To provide proper security for the data; To determine the required retention period of the data; and to ensure proper disposal of the data. (E.C. 5.2).

When we learned that Equifax keyed the data to the Social Security Number we stepped up our efforts to oppose the release of the product. In January of this year CPSR announced its formal opposition to the release of the product. Shortly afterward, Lotus and Equifax held a press conference and cancelled the release of Marketplace.

We were pleased that Lotus chose to cancel the product. This was a significant privacy victory that served the best interests of American consumers. The defeat of Marketplace has also opened the door on an industry practice that should be curtailed.

Let me now explain the problem with the use of Social Security Numbers for records management.

USE OF UNIQUE IDENTIFIERS IN COMPUTER DATA BASES

Every system of records requires some type of index to ensure that individual records can be retrieved. Although alphabetizing may work for small record sets, such as the names of students in a grade school class, such a system will quickly collapse as the size of the group increases.

Organizations therefore develop numbering systems to help identify records regarding their customers. These account numbers help a company locate a specific record when an inquiry is made, a transaction is posted, or an account is modified. They also allow a customer to verify charges and to make inquiries.

There is no necessary reason that companies should use the same numbering schemes. In fact, in the Washington, DC area, the gas company uses one account number system, while the utility company uses a second numbering scheme, and the phone company a third. Though each numbering system shares the common characteristic that a particular account number identifies a unique record.

Some private sector companies have found that the development of personal identifiers that are not based on the Social Security Number may actually be more useful for the organization. For example, some code numbers include information about the individual, such as expiration date for a subscription or a zip code from a mailing address. Unique identification codes are also relatively easy to develop.

THE SOCIAL SECURITY NUMBER RAISES SPECIAL PRIVACY PROBLEMS

The central problem with the use of a Social Security Number as an identifier is that it allows organizations to obtain information about individuals with whom there may be no prior relationship. This tends to diminish an individual's ability to control information about himself or herself and leads to the compilation of elaborate dossiers often without the knowledge of the individual.

When an individual discloses an account number to a particular business or institution, the information that is disclosed is only that necessary to identify the person to the particular institution. The disclosure of personal information to a particular company for a specific purpose establishes an expectation of confidentiality.[3] Numbering schemes that are designed for particular businesses help promote confidentiality because they strengthen the ties between the individual and the institution and create an expectation that information which is transferred to the institution will not be used for other purposes.

Similarly, single-purpose identification cards without universal identifiers, such as SSNs or PINS,[4] can actually enhance personal privacy by restricting the extent of a person's identity that must be disclosed to interact with a large institution. Library cards and driver's licenses are examples of such limited purpose cards. In those information systems, privacy protection should focus on the subsequent use of the information by the information-holding institution, but the card by itself is unlikely to create a privacy problem.

Multi-purpose identification numbers for which the purpose is open-ended may be more problematic. An institution that obtains the number presumably will have access to all the information that the document holder would have. This access allows the institution to create more elaborate picture of the document-holder than the single-purpose document.

---

[3] Report of the Privacy Protection Study Commission (1977).

[4] Personal Identification Numbers (PINs) refer to any identity number associated with a card. In the United States, an individual may have many PINs: a bank ATM card, a telephone charge card, a workplace access card. In other countries such as Sweden and Australia, the term "PIN" is often used to refer to a universal tax number, similar to the social security number (SSN) in the United States, and therefore raises much of the same concern as the SSN.

As Congressman Frank Horton said almost twenty-five years ago:

> One of the most practical of our present safeguards of privacy is the fragmented nature of personal information. It is scattered in little bits across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard.[5]

If the Social Security Number became a national identifier and were routinely used in commercial transactions, the expectation of confidentiality that is created between an individual and an institution would be undermined and the opportunities for the unauthorized transfer of personal information would increase dramatically.

RESTRICTIONS ON THE USE OF THE SOCIAL SECURITY NUMBER

The privacy problems with the misuse of the Social Security Number were set out in a landmark 1973 HEW report titled Records, Computers, & The Rights of Citizens. The HEW report recommended that:

- Uses of the Social Security Number be limited to only those purposes required by the federal government.
- Federal agencies should not require the use of the Social Security absent statutory authority.
- Congress evaluate any proposed use of the Social Security Number
- Individuals have the right to refuse to provide their Social Security Numbers, and should suffer no harm for exercising this right.

---

[5] "The Computer and the Invasion of Privacy," Hearings before the Special Subcommittee on Invasion of Privacy of the Committee on Government Operations, House of Representatives, 89th Cong., 2d Sess. 6 (1966)

- Organizations required by Federal law to obtain the Social Security Number use the number solely for the purpose for which it was obtained and not make any secondary use or disclose the Number without the informed consent of the individual

In 1974 Congress adopted many of the recommendations of the HEW report and made clear that the use of the Social Security Number should be restricted. The Privacy Act of 1974 said specifically that:

> It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. (7)(a)(1).

The Privacy Act further said that:

> Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it. (7)(b).

This means that any federal agency which requests an individual's social security number is required to (1) cite its formal legal authority for using the number; (2) reveal whether disclosure is mandatory or voluntary; and (3) explain how the number will be used.

TECHNICAL SOLUTIONS.

I should also mention a technical approach to the problem of privacy protection. It is possible to develop a system based on digital signatures that would allow individuals to conceal their actual identities while providing enough information to complete transactions with businesses. This system would frustrate cross-matching between different databases and restrict the disclosure of information to that which is necessary for the transaction.[6]

---

[6] David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM (October 1985); Office of Technology Assessment, Defending Secrets, Sharing Data: New Locks and Key for Electronic Information (1987); David Chaum and Jan-Hendrisk Evertse, "A Secure and Privacy-Protecting Protocol for Transmitting Personal

Such a system would allow individuals to create their own pseudonyms rather than to have them issued by the sponsoring institution. It would also be possible for individuals to control the records of transactional information, which would make it easier to correct and modify personal information.

RECOMMENDATIONS

Mr. Chairman, there is no necessary reason that the widespread misuse of Social Security Numbers should continue. Reasonable alternatives exist for organizations to manage their record systems. Continued reliance on the Social Security Number will simply undermine expectations of confiedentiality and privacy safeguards.

CPSR recommends that Congress develop legislation that would prohibit the collection and use of Social Security Numbers were not required by law. We propose fines and sanctions for companies that seek to obtain the Social Security Number without explicit statutory authority.

We also recommend that the legislation require organizations that request the social security number to comply with the same standard that was established for federal agencies by the Privacy Act of 1974. Companies must (1) provide clear legal authority for using the number; (2) reveal whether disclosure is mandatory or voluntary; and (3) explain how the number will be used. Any organization that fails to satisfy these goals shall be required to pay a stipulated damage award to the person whose social security number was wrongfully obtained.

CPSR further recommends that the Social Security Administration not be permitted to transfer social security records to any third parties or to use social security records for purposes unrelated to the original collection. Such uses may well be prohibited bu the Privacy Act of 1974.

CPSR also recommends that the Committee identify those instances where the disclosure of the Social Security Number is currently required by law and then determine whether alternative schemes might be available to manage these record systems.

Information Between Organizations," Advances in Cryptography: Proceedings of Crypto 86 (A.M. Odlyzko ed.)

Mr. Chairman, I recognize that these are strong measures. However, such steps taken at this point would be an appropriate "mid-course" correction. The legislation would allow organizations to continue to make use of automated information systems without compromising individual privacy.

Almost twenty years to this day MIT President Jerome Weisner testified before Senator Sam Ervin's Committee on the need for strong privacy measures. Professor Weisner stated:

> It is obvious that means for effective record-keeping, information gathering, and data processing are essential needs of a modern society. The problem for us is to determine how to reap the maximum assistance from modern technology in running a better society and at the same time, how to keep it from dominating us. In order to do this we may need to adopt some stern measures in the form of very strict controls on who can do what with private information about any individual in the society.[7]

I hope that the Committee will take Professor Weisner's good advice and support these proposed restriction on the use of the Social Security Number.

That concludes my testimony. I would be pleased to answer your questions.

---

[7] Federal Data Banks, Computers and the Bill of Rights, Senate Judiciary Committee 1971

Chairman **Jacobs**. Thank you, very much.

No questions.

Your testimony was very crisp and yours is very informative and we are very grateful.

Thank you.

The next panel consists of Mr. Rothfeder, Mr. Wiggins, and Mr. Connelly. Advance and be recognized. We will take a moment here to do some identification.

Mr. Rothfeder.

STATEMENT OF JEFFREY ROTHFEDER, FORMER INVESTIGATIVE REPORTER, BUSINESS WEEK MAGAZINE, AUTHOR OF NO SECRETS, WYCKOFF, N.J.

Mr. **Rothfeder**. My name is Jeffrey Rothfeder and I am an investigative reporter and for the last few years I have been covering data banks and computer technology. One thing that has become clear is that the Social Security number has become a national ID and I don't have to go into all the agencies that are allowed to use it and all the bureaus that are allowed to use it.

What I would rather talk about though is that the unchecked use of the Social Security number within the private sector mainly has led to a problem of massive proportions. Quietly people with checkered motives are turning easy access to Social Security numbers into an epidemic of financial scams, invasions of privacy and unregulated mischief that is only getting worse. Computer technology has made it worse, basically because now you can buy computers that are the size of what mainframes were 20 years ago and you can put them on your desktop at home and buy them for under $2,000. And data banks are proliferating.

Information about every move we make, whether we buy a car or a home, apply for a loan, take out insurance, purchase potato chips, request a Government grant, pay taxes, get Social Security, go to work, see a doctor, is fed into dozens and dozens of data banks. That is the natural course of our business. And then from these data banks, information is broadcast out onto a lower level of data banks, which either work for the original company that accessed the information or resell it out to consumers or out to people who want to know.

And I see it as a bulging pyramid of information and Social Security numbers travel freely throughout it, bouncing from one computer to another and with little attempt to hide it from anybody who wants to snoop. And let me tell you how easy it is to get someone's Social Security number.

First of all, you could go on any one of hundreds of information resellers and ask for the top part of a consumer credit report which is called a header and that is legitimate to get basically because it is the way that you tell who you are going to get a credit report on. So under the Fair Credit Reporting Act that's legitimate to get and within minutes I can basically get anyone's Social Security number that way.

Last year I got a famous Social Security number when I obtained the copy of Dan Quayle's credit report. And I got it from my computer at home and I purchased it from a data bank, not from one of the big three credit bureaus, because their security is a lot tighter. I purchased it from somebody who has lax security and is willing to sell this information to anybody.

I never compromised Quayle's privacy, by the way. I never published any information from his credit report and I have never disclosed it to anybody. But now I had his Social Security number and it gave me—the question could be what is the harm in that? What could I do with it? Well, basically it gave me the right to continue to tail Quayle. It allowed me to learn more about the Vice President as I wanted to.

I can give you a good example of this, using Dan Quayle as a test case. I called up—I did not have his current address or phone number, because this was an old credit report. So I called up Sears where he has a charge account, and I said to them that I am from Chrysler Credit in New Jersey and I have an application from somebody for an auto lease but he did not put his current address and telephone number on there. Could they give me this information?

And the guy said, sure. I would be glad to help, what is his account number? So I gave it to him. And then he came back and said, wait, that is Dan and Marilyn Quayle's account. And he was real suspicious of me, which he should be.

And so I put him at ease and I said to him, I know it is their account but I have got to process this application and nobody in the Vice President's office will help me out. He left this information out and could you please help me?

Then I let loose with the guns, I said, look I can give you his Social Security number if you need proof that he actually filled out this application with us. That cut right through his skepticism. I gave him the Social Security number and it matched up with what was on the record, and then he gave me his address and he gave me his phone number and I said, thanks a lot, you have been a big help. And he said, well, wait a second. This is an unpublished address and phone number so don't pass it around to anyone. [Laughter.]

And I said, of course, I won't do that.

Now, I am not dangerous but others are, and they can use this information in blackmail, larceny, or voyeurism. And there are some real cases of this going on. Law enforcement officials in every major city tell me that these types of incidents are increasing in frightening numbers.

For instance, there are organized crime units using Social Security numbers and names obtained from data banks to give illegal aliens legitimate identities to get jobs in the United States. Then they don't pay taxes and the original person whose name is being used, gets caught by the IRS a few years later and has to get himself out of that mess.

There are also gangs, mainly foreigners living in the United States who are applying for credit cards and loans from banks based on Social Security numbers that they have again, obtained illegally and banks are not checking up any more and savings and loans are not checking up because their profit margins are down the tank and they just want to give the loans out as much as they can.

So, in conclusion, I don't think Congress can take away from the credit bureaus and the other guys the right to use the Social Security number now, because they would have to rejigger their systems and it would cost millions and millions of dollars and the consumer would be hurt. I mean you gave them the right many, many years ago and it is hard to take it away now.

What I would say that would make sense is if companies like the banks and others don't check on the applicants that are coming in, don't do a further check than just do you have a Social Security number, or Sears doesn't check on me before giving me Dan Quayle's name and address then they should be held liable. And if I abuse Quayle's privacy he should be able to sue Sears for giving out that information. I mean somebody has to have a liability for this.

Thank you.

[The prepared statement follows:]

TESTIMONY OF JEFFREY ROTHFEDER BEFORE THE HOUSE SUBCOMMITTEE ON SOCIAL SECURITY

Mr. Chairman, and members of the Committee:

Gradually the social security number has become nothing less than a national I.D. And the federal government has only itself to blame. The Social Security Administration and Congress has directly or tacitly allowed this to happen with virtually no resistance. It's occurred slowly, over nearly sixty years, but now the social security number, which was once sacrosanct and private, is used by dozens of companies and government agencies--among them, credit bureaus, banks, schools, motor vehicle agencies, employers, and insurers--as the prime identifier distinguishing one record from another in their massive computer systems.

And you can't blame them for doing so, given the opportunity. Everyone has a social security number. And when you're storing millions of files on Americans as many of these organizations do, the social security number is the most efficient way to separate one John Smith from the hundreds of others in the system, assuming, of course, that the typos are kept to a minimum. What's more, when one computer needs to pull files from its counterpart at another organization, standardized numbering using social security numbers ensures that the correct records are retrieved. Indeed, in a perfect world, it's probably a good system. But that's not the kind of world we live in.

Instead, unchecked use of the social security number in databanks has led to a little understood problem of massive proportions. Quietly, people with checkered motives are turning easy access to social security numbers into an epidemic of financial scams, invasions of privacy, and unregulated mischief. And it's only getting worse.

That's because of the technology explosion. Computers the size of a notebook are now as powerful as those that once filled rooms in corporations, and are available to anybody for less than $2,000. And with this has come a boom in databanks for sale. Information about every move we make--buy a car or a home, apply for a loan, take out insurance, purchase
potato chips, request a government grant, pay taxes, get social security benefits, go to work, see a doctor--is initially fed into dozens and dozens of separate databases owned by the government, the Big 3 credit bureaus, banks, insurance companies, marketers, schools, employers, among many others. And from these databases this information is broadcast to thousands of regional databanks, and frequently to information resellers in New York, Peoria, Kankakee, and everywhere else. Finally, the data is shipped to the millions of easily accessible computers on corporate desktops or in people's homes throughout the country.

It's a bulging pyramid of information. And social security numbers travel freely throughout it, bouncing from one computer to another, with little protection from those with the bent to snoop. And because social security numbers are perceived as the most private of numbers--even if in practice they're not anymore--when you know someone's number, as I will show, malevolence can follow.

Want to know how simple it is to get someone's social security number? The easiest way is to retrieve a so-called credit report header on him. That's the top part of a consumer credit report--it contains no personal financial information, but usually lists a social security number. And it's legitimately available to anybody, because it's not covered by the Fair Credit Reporting Act. Headers can be purchased via computer from any one of hundreds of information resellers, and through them within minutes in my office I can get anybody's social security number in the United States.

Last year, I got a famous one when I went further than just the header and obtained a copy of Dan Quayle's full credit report. I accessed it on a Macintosh computer, purchasing it from a databanker that subscribes to the Big 3 credit bureaus and whose security is so lax that it freely sells credit reports to virtually anybody who asks for one. I did it as a journalistic exercise. I wanted to show that with privacy at a premium and databanks proliferating even the Vice President of the United States is easy pickings for somebody with prying eyes. By the way, I never compromised Quayle's privacy: I have never published and have never disclosed to anyone the personal details contained in the Vice President's credit file. But now that I know Dan Quayle's social security number, and other private information about him, what's the harm? What can I do with it?

Plenty. Simply put, this gives me the right to continue to tail Quayle; it allows me to learn even more about the Vice President and update what I already know about him whenever I want to and at will. That's because being privy to the Vice President's social security number, credit card data, address, and salary, in the parlance of databanks, makes me an intimate of his--and gives me free access to more information (what could be wrong, goes the reasoning? He knows, therefore, he can know).

Let me give you an example of how this works, using Dan Quayle, again, as the test case. The credit report I had on Quayle didn't contain his telephone number and the only address it listed was his home in Indiana. I wondered if he also had a house in the Washington, D.C. area. So I called up Sears credit department, where he has an account, and told the clerk who answered that I was from Chrysler Credit in New Jersey and that I have an application from somebody for an auto lease, but the applicant failed to put in his current address and telephone number. "Could you," I asked, "help me out with this information?"

"Be glad to help. What's his Sears account number?"

I supplied it.

Over the phone I heard him typing it into his terminal. "That's Dan and Marilyn Quayle's account," the clerk said slowly, suspiciously Q as if to say, hey buster, what the heck are you up to and what illegal act are you trying to get me to perform? I knew I had to put him at ease immediately. I had to quickly produce my Quayle insider passport and prove that this was a data channel that I was authorized to be on. "I know that it's their account," I said, chuckling embarrassedly. "But I'm only a clerk here and I have to process this application. And nobody in the Vice President's office will help me out. For some reason, he handed in an application without filling in all the blanks."

Then I let loose with my big guns. "I can give you his social security number, if you need proof that he actually filled out an application with us," I said.

That cut right through his skepticism. How could I be an imposter if I had in my hands such a private piece of data?

"What social security number do you have for him?" the clerk asked.

I read it to him and it matched what was on his computer screen at Sears. The floodgates were opened. "The local address we're showing is XXXX in McLean, Virginia," the clerk said.

I gingerly took the next step. "Do you have his phone number?"

"Sure. 703-XXX-XXXX."

"Thanks a lot. You've been a big help."

But he wasn't through. "Oh, by the way. This is an unpublished address and phone number, so don't pass it around to anyone."

"Of course," I said.

Now I'm not dangerous--but others are. And they can get his and anyone else's social security number just as easily. And use it against victims in complex webs of blackmail, larceny or voyeurism that can even lead to threats on their lives or worse. Indeed, during reporting for my upcoming book, "No Secrets" I've found dozens of cases in which criminals are using the easy availability of the social security number to commit a growing number of crimes against property and privacy--a fundamental right of Americans. And law enforcement officials in every city tell me that these types of incidents are increasing in frightening numbers. Two examples:

o Organized crime units are using social security numbers and names obtained from information resellers' databanks to give illegal aliens legitimate identities with which to get jobs in the United States. And not pay any taxes. Problem is, when the IRS discovers the scam, the victim--the person's whose social security number was used--becomes the guilty party and is forced to spend months and thousands in legal fees undoing the mess.

o Gangs--mainly foreign nationals living in the United States--are applying for credit cards and collateralized loans with illegally obtained social security numbers and making off with millions in stolen merchandise and embezzled money sent to maildrops. By the time the scheme is uncovered, these con-artists are long gone, and the person whose name is on the credit card or bank check is left holding the bag.

Clearly, we're paying mightily today in personal and corporate injury from the widespread use of the social security number, which began in the pre-dawn of the computer age, years before databanks were everywhere and information-for-sale companies were endemic.

But there's little that Congress can do about it now. It would be an expensive and unfair penalty to withdraw from the private sector and others the right to use the social security number as an identifier. The costs of rejiggering the computer systems would reach into the hundreds of millions of dollars. And it would be hypocritical of Congress to do this, while the Social Security Administration participates in dozens of computer matching programs, in which its internal data is shared with other government agencies and companies to ostensibly catch people double-dipping the government or embezzling from the private sector.

Perhaps what would make more sense would be to hold companies and government agencies responsible for criminal and civil liabilities when they give out personal information--be it medical records, personnel files, or household data--loans or credit without an acceptable background investigation. For the purposes of this discussion, that means without looking any further than if the requester provides the correct social security number matched against a given name. These organizations should know better than to allow this. They use the social security number freely in their systems. And they're aware that in this computer age every one of their employees earning $12,000 or $120,000 can access at their desks in seconds the social security numbers of thousands of people with just the press of a button. With that kind of knowledge, the private sector and the government shouldn't treat the social security number as the ultimate ticket to private information and financial gain, obtained at some unknowing victim's expense.

Chairman JACOBS. Mr. Wiggins.

STATEMENT OF JAMES R. WIGGINS, JR., WASHINGTON, D.C.

Mr. WIGGINS. Thank you.

I am James Wiggins and I am involved in a multimillion dollar lawsuit against a private vendor, Equifax Services. My Social Security number was used in a way to lend authenticity to a false, altered report and furnished to my employer, District Cablevision by Equifax, Inc.

My Social Security number was used to indicate the conviction of myself on a felony cocaine conviction. I have no record and I have no criminal conviction. Equifax uses Social Security numbers to sell information regardless if it is true or false to ruin my life. I am presently now in the court system, in Federal Court with Judge Michael Boudin, a new Federal Judge and hopefully my case will help hundreds of other people who have this kind of report going out nationwide, worldwide. And have no knowledge that it is being reported, through the Social Security number.

Basically, I don't want to say too much more because it is presently in court, but I will definitely answer any questions. You have my testimony.

Thank you.

[The prepared statement follows:]

TESTIMONY OF JAMES R. WIGGINS, JR.

In January 1990, James R. Wiggins, Jr. was fired by District Cablevision after a wilful and deliberate criminal records check by an Equifax Services, Inc. employee. A suit is pending against Equifax Services, Inc. and one Supervisor, Darrell J. Madden.

Liability against Defendant, Equifax Services, Inc. ("ESI") for wilful and deliberate violations of the Fair Credit Reporting Act, under 15 U.S.C. § 1681 (e)(b) and 15 U.S.C.A. § 1681 (k) are based on the corporation's failure to follow strict procedures or reasonable procedures to assure maximum accuracy of a criminal records check.

District Cablevision, the former District of Columbia employer of James R. Wiggins, Jr. requested a criminal records check on James R. Wiggins, Jr. The request was made by fax dated January 2, 1990, sent (originating) from the Cleveland, Ohio Equicenter to the Washington office of ESI, actually located at 8180 Greensboro Drive, McLean, Virginia.

On January 3, 1990, Ms. Tami Plumer, a part time Field Representative (investigator), who is a Virginia resident, phoned a deputy clerk in the criminal division of Superior Court for the District of Columbia and gave the female clerk, whose name was not known to Ms. Plumer, the name "James R. Wiggins" for a criminal records check! The clerk quickly stated that James R. Wiggins had a conviction and Ms. Plumer claims she gave Mr. Wiggins' birth date as March 17, 1954, which has not been verified. Plaintiff relies on Pages 37 thru 41 and other parts of the transcript of Ms. Plumer's deposition testimony, which was given in Fairfax, Virginia on January 3, 1991.

In the ensuing conversation on January 3, 1990 between Ms. Plumer, a regular employee of ESI, and the deputy clerk in the criminal division, Ms. Tami Plumer wrote in her notes that:

1. James R. Wiggins had a conviction for Possession of Cocaine, which was false.
2. That James R. Wiggins was "tried and found guilty." (False also)
3. That James R. Wiggins' conviction was a "State Felony." Each of the facts 1-3 is false, even as to James Ray Wiggins,[1] who was born December 15, 1963. (See, Plaintiffs' Exhibits 2-4 which are exhibits from the deposition of Thomas Shaw, an ESI Manager that appears in the Court file (CA 90-199).

All of the information recorded above (1-3) by Ms. Plumer was transmitted by telephone to Mr. Roderick David Williams, a full time employee of ESI, and a principal assistant to Ms. Sally Ann Myers, records supervisor at ESI, and was recorded on an ESI FAX form by Mr. Roderick Williams.

Later on, or about January 5, 1990 the ESI FAX form with the false James R. Wiggins data was faxed to the Cleveland, Equicenter of ESI in Cleveland, Ohio. The Cleveland office of Equifax (Mrs. Ruth Sopata) telephoned the false information (felony cocaine conviction, etc.) to Miss Cynthia Lee at District Cablevision.

On, or about January 10, 1991, Mr. James Russell Wiggins, Jr. denied to a District Cablevision official, Mr. Allen Rogers that he had any criminal conviction and made further denial that the data in Plaintiffs' Exhibit 3 did not pertain to James R. Wiggins, Jr.

Ms. Cynthia Lee, Human Resources Director at District Cablevision discussed denial by James R. Wiggins, Jr. with Miss Ruth Ellen Sopata ("Ruth Sopata") in the Cleveland Equicenter of ESI on or about January 10, 1990 and after James R. Wiggins, Jr. made his denial and made a request for reinvestigation to Ms. Sopata in the ESI office in Cleveland, that was sent to the Washington office of ESI on January 10, or January 11, 1990 by Pat Anderson of the ESI Cleveland, Ohio office by phone and by fax and was transmitted directly to Sally Ann Myers, Records Supervisor in the Washington office of ESI on January 10 or 11, 1990.

On January 12, 1990 Tami Plumer went to Superior Court for the District of Columbia, Room 4001, to the Criminal Clerk's office and ordered part of the criminal file of James Ray Wiggins, born December 15, 1963, ordered by Docket No. F 14105-88. Ms. Plumer requested the deputy clerk of Superior Court to copy certain selected pages.

The print out of the James Ray Wiggins Criminal Index reference as it appeared on the Supreme Court computer screen on January 3, 1990 is in the Court record (CA 90-199).

Mr. Roderick Williams testified during his deposition on November 14, 1990, that ESI changed its procedure after the James R. Wiggins suit, so that when a "hit," i.e., a conviction is indicted by a criminal clerk of the Superior Court in response to a telephone request by an ESI employee then, and only then, ESI picks up a "hard" copy of the criminal conviction documents from the Superior Court file and not necessarily the whole criminal file from Superior Court, just as was done in the James Russell Wiggins case on January 12, 1990 by Ms. Tami Plumer and the conviction documents are reviewed by Sally Myers' office at ESI in McLean, Virginia.

Several witnesses, including Roderick D. Williams and Sally A. Myers and Ms. Plumer have acknowledged that ESI has changed its procedure since the James R. Wiggins law suit, so as to have the ESI field investigator obtain a "hard" court copy of any criminal conviction before transmitting information to an employer so that ESI can check the identity of the convicted party.

In this case, Defendant, Equifax Services, Inc. did on January 3, 1990 wilfully and deliberately violate 15 U.S.C.A. § 1681 (e)(b) and 15 U.S.C.A. § 1681 (k) in that an Equifax Services, Inc. employee, field representative, Tami Plumer did not "follow a reasonable procedure to assure maximum possible accuracy of the criminal records information" concerning James R. Wiggins, Jr. born March 17, 1954, and failed to follow strict procedures in that a telephone call was made to the

---

[1] James Ray Wiggins had made a plea of guilty to attempt to possess cocaine and was given probation without judgment of guilt -- which is not a criminal conviction!

Superior Court Criminal Clerk's office on January 3, 1990 and that the clerk made a report to Tami Plumer, the authorized agent of ESI, working within the scope of her employment that the information was recorded in written notes by Tami Plumer and was later reported again by phone to Roderick David Williams, the assistant to Sally Ann Myers, who is the Records Supervisor in the McLean, Virginia office of ESI, that James R. Wiggins born March 17, 1954 had a criminal record for cocaine possession (felony) and was found guilty after a trial. Each of these important facts are set forth in Plaintiffs' Exhibit 3 which are incorrect and totally false even as to James Ray Wiggins, born December 15, 1963 the person actually charged with a crime, who later was given probation without judgment.

Let me point out that the stated facts, as set forth above are taken from the deposition testimony of Tami Plumer, who is the former employee of Equifax Services, Inc. who investigated the James R. Wiggins criminal records check, and Roderick David Williams, the Assistant to Sally Ann Myers, Supervisor of Records in the Washington office of ESI (McLean, Virginia)!

The facts set forth (Plaintiffs' Exhibit 1) all in the hand writing of Roderick David Williams, were reported to Mr. Williams by Ms. Tami Plumer and each fact set forth in the report is partly or completely false and resulted from a telephone report made by an alleged unknown clerk of the criminal division of Superior Court in a telephone conversation with Ms. Plumer on January 3, 1990.

(Plaintiffs' Exhibit 3 shows that) James Ray Wiggins was a youthful offender who made a plea to a misdemeanor, i.e., attempt to possess cocaine under Title 33 D.C. Code § 541 (e) and was given probation without judgment of conviction. In such a case there is no finding of guilt and no judgment of conviction as set forth by the D.C. Court of Appeals in U.S. v. [illegible]ty, 541 A.2d 612. Here, there was no conviction, no felony and no finding of guilt of any one, and certainly not James R. Wiggins, Jr.

Section § 1681 (k) of the F.C.R.A. entitled, Public Records Information for Employment Purposes, Section (k) provides:

> A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose complies and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment shall:
>
> (1) at the time such public record information is reported to the user of such consumer report notify the Consumer of the fact that public record information is being reported by the consumer reporting agency together with the name and address of the person to whom such information is being reported; or
>
> (2) maintain strict procedures designed to insure that wherever public records information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date.
>
> Records, arrests, indictments, and convictions are items of public record included under this paragraph.

The record is clear that the ESI report contains grossly inaccurate statements of the public record as to the D.C. Code Title 33 - 541 (e) plea by James Ray Wiggins born December 1963, to a misdemeanor and with probation and sentence of 12 months without judgment, that is clearly not a conviction; no felony conviction and no trial or entry of judgment. In addition, Equifax did not (1) report to Plaintiff, James R. Wiggins under k(1) and did not maintain strict procedures to comply with Paragraph k(2) of the FCRA even as to the wrong James R. Wiggins, born December 15, 1963. The report, made by Equifax is clearly erroneous and does not measure up to the statutory strict procedure required for reporting public record information on arrests and convictions.

An agent or employee of Defendant, ESI negligently, and wilfully copied the felony criminal, charges (not a) conviction record of one James Ray Wiggins. Later, after deliberate and willful modification and alteration, Defendant ESI published and furnished this criminal conviction with James Russell Wiggins' correct social security number and correct birth date and correct address to be an indication of the conviction of Plaintiff James Russell Wiggins on a felony cocaine conviction. Plaintiff James Russell Wiggins has no criminal conviction.

Upon information and belief, Plaintiff James Russell Wiggins alleges that the photocopies and other facsimiles of copies referring to the James Ray Wiggins' criminal conviction were modified, altered and amended by Defendant ESI to show as a part of the same record, the accurate and correct birth date of Plaintiff James Russell Wiggins, and the correct social security number and other data were added to the James Ray Wiggins' felony conviction records for cocaine possession (felony).

Upon information and belief, Plaintiff, James Russell Wiggins alleges that the true accurate and correct social security number and the home address of Plaintiff James Russell Wiggins were added and appended to the James Ray Wiggins' felony criminal conviction report in a way to lend authenticity to the report furnished to District Cablevision on January 17, 1990.

Clearly I, James Russell Wiggins, Jr., am having difficulty finding gainful employment in the District of Columbia, even though I am a presentable college graduate. (A study once showed that 75 per cent of employment agencies will not place a person with an arrest record, never mind a conviction, never mind a drug violation) according to the Privacy Journal, June 1990.

James R. Wiggins, Jr.
Testimony
February 27, 1991

I, James Russell Wiggins, Jr., have no idea when the erroneous and altered employment report will return to haunt me. I, am an African American like most persons victimized by Consumer Information company mistakes. Even when wilful and deliberate such disinformation can continue to re-appear throughout one's life in the revised form of electronic, and so far, legal lynching. Moreover, many if not most persons stigmatized by erroneous criminal misinformation, and/or disinformation are black, and most times financially and socially unable to seek immediate, and/or long term justice and relief through the American court systems. Again, even when wilful, and deliberately false information is uninhibited, it may appear, and reappear when Vendees from anywhere are able to buy such mistake ridden disinformation from Equifax on a daily basis.

Equifax Services, Inc., the largest supplier of investigative reports on employment applicants, takes information on criminal records from court sources by telephone and then passes it on to employers, again by telephone, without verification, according to Publisher Robert Ellis Smith, in the Privacy Journal. He also authored a followup story in the recent publication of Privacy Journal, January 1991, where the article signals a possible FTC violation by ESI.

In addition, the FCRA requires a higher standard of "strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported is complete and up to date". A Federal Trade Commission enforcement officer has expressed surprise that Equifax gathers and reports criminal information by telephone.

The employment damages in this case are overwhelming and have caused great family hardships including lost wages.

In addition, James R. Wiggins, Jr. and his wife have suffered emotional distress that has required medical attention. Dr. William Milton, III a dentist has stated (Quote affidavit)

1. I am a dentist/surgeon licensed in the District of Columbia for many years and I specialize in the practice of dental surgery.

2. I attended to both Mr. James R. Wiggins and Mrs. Kashimu Wiggins in January 1990 and continue to do so, to date.

3. It is my opinion that Plaintiff James R. Wiggins and his wife, Kashimu Wiggins have suffered continuing stress from mid-January 1990 to date. Mr. Wiggins was diagnosed as requiring a mouth retainer prothesis to reduce various symptoms due to the level of stress from which he is suffering, as well as Mrs. Kashimu Wiggins requiring treatment for evidence of an unusual level of ever increasing stress resulting in her grinding of teeth due to the circumstances occurring in January 1990 and until present time.

Treating medical doctor, Augustus Hill is licensed to practice medicine in Maryland and specializes in surgery.

Dr. Hill filed a statement with the court concerning damages from physical stress and anxiety and performed a surgical procedure for stress on James R. Wiggins, Jr. on December 27, 1990 in relation to his physicial condition due to stress.

I, James R. Wiggins, Jr. have undoubtedly suffered from the deliberate and intentional accusations of a Felony Cocaine Conviction that amount to lible, per se and an unwarranted attack on my reputation.

James R. Wiggins, Jr.

By Counsel:

John C. LaPrade-Bar No. 171.389
Attorney for Plaintiffs
1730 K Street, N.W. - Suite 304
Washington, D.C. 20006
Tel.: (202) 328-3350

Frazer Walton, Jr.-Bar No. 374301
Attorney for Plaintiffs
526 King Street - Suite 413
Alexandria, VA 22314
Tel.: (703) 683-1318

Chairman JACOBS. We thank you, Mr. Wiggins.
Mr. Connelly.

STATEMENT OF D. BARRY CONNELLY, EXECUTIVE VICE PRESIDENT, ASSOCIATED CREDIT BUREAUS, INC.

Mr. CONNELLY. Thank you, Mr. Chairman.

My name is Barry Connelly and I am the executive vice president of Associated Credit Bureaus, the trade association representing the consumer credit reporting industry. ACB, as we are known in the industry, represents over 900 member bureau offices in the United States, including the three automated repositories, Equifax, TRW, and Trans Union.

We appreciate the invitation to describe the credit reporting industry usage of the Social Security number. It is very important during any discussion of the credit reporting industry to remember that as a private sector data base it is strictly regulated by the Fair Credit Reporting Act. The Fair Credit Reporting Act holds consumer credit reporting agencies to a standard of following reasonable procedures to assure maximum possible accuracy of the information reported. It is in compliance with this Federal requirement that the Social Security number is important.

The mission of the consumer credit reporting industry is to provide accurate credit histories in the form of accurate consumer reports to credit granters to facilitate consumer transactions. This service fuels the U.S. economy and it makes it possible for your constituents to buy homes and cars and goods and services with relative speed and ease.

Consumers, in the interest of obtaining credit, are very anxious that lenders see their entire credit history. Credit granters, in the interest of making the sale and receiving payment, depend on the credit reporting industry to provide them with fast, accurate information on which to make the credit decision. The Social Security number enhances the credit bureau's ability to provide a complete and accurate credit history file on the consumer to the credit granter.

It is used to merge files, to prevent the merging of wrong information into one file and to locate files that could not otherwise be retrieved based on names and addresses. The credit bureau obtains the consumer's Social Security number in three ways. If a credit granter making an inquiry about a consumer includes the number in the inquiry process it is captured at that time.

Second, credit granters contribute their customer credit history to the consumer reporting agencies each month by automated tape. If the number is included at that time, the credit bureau captures it at that moment.

The third method is when consumers, themselves, provide the number voluntarily to the credit bureau. Credit bureau file structure is primarily based on name and address, but other identifying elements of information are used, including Social Security number, former address, date of birth, and generation code.

The full credit report is not accessible to subscribers who inquire with only the Social Security number. As we have all experienced our name or address is often given in different or varying ways. My birth certificate, for example, identifies me as David Barry Connelly, however, I find that I am variously known by my creditors as D. Barry Connelly, D.B. Connelly, Barry Connelly, David B. Connelly.

The use by credit bureaus of the Social Security number compensates to a very great extent for the inconsistent, inaccurate, and nonunique use of name and address identifiers, because it enables credit bureaus to find more of the consumer's credit history and it enables the bureaus to distinguish between consumers who have or use similar or identical names or addresses.

We caution, however, that the Social Security number is not a panacea for accuracy. But inability to use the Social Security number as an identifier would only result in lessening the ability of the consumer reporting industry to meet the congressional mandate of the FCRA. ACB believes that consumers and credit granters would suffer the consequences of less accurate and complete information being available.

The Fair Credit Reporting Act limits access to the information in our member files only to those with a permissible purpose as defined by law. Credit bureaus are required to obtain certification from users, that the information will only be used for a lawful purpose and that is usually done by a signed contract. An individual must lie and consciously violate the FCRA to obtain information without a permissible purpose.

In conclusion, the members of the Associated Credit Bureaus are attempting to achieve that delicate balance between a congressional mandate to report with maximum possible accuracy and the legitimate concern we all share over unwarranted invasion of personal privacy.

We desire only to be good corporate citizens, and provide an indispensible service for the economic health of this country. We do not seek to be part of any one large information network. We believe that our use of the Social Security number as described provides more benefit than any perceived threat to American consumers.

With that, Mr. Chairman and members, I will be happy to answer any questions.

Thank you.

[The prepared statement follows:]

TESTIMONY OF D. BARRY CONNELLY
ASSOCIATED CREDIT BUREAUS, INC.

Mr. Chairman and members of the Subcommittee on Social Security, my name is Barry Connelly and I am Executive Vice President of Associated Credit Bureaus, Inc., the international trade association representing the consumer credit reporting industry. Our headquarters is in Houston, Texas.

ACB, as we are known in the industry, represents over 900 credit bureau member offices in the United States. Nearly 600 of those offices are automated while just over 300 operate on a manual basis. Our membership includes the three automated repositories, Equifax Credit Services, TRW Information Services, and Trans Union Corporation. Each of these companies have affiliated contracts with 467 independently owned credit bureaus across the country. Each company claims to maintain credit history files on over 150 million consumers. Last year, we estimated that approximately 450 million credit reports were issued in the United States.

We appreciate the invitation to appear before the subcommittee and the opportunity to describe the credit reporting industry usage of the social security number. Our members are particularly sensitive to the privacy issue and are justifiably proud of our support of and compliance with the Fair Credit Reporting Act (FCRA). It is important during any discussion of the credit reporting industry to remember that as a private sector data base it is strictly regulated by the FCRA.

The Fair Credit Reporting Act also holds consumer credit reporting agencies to a standard of following "reasonable procedures to assure maximum possible accuracy of the information" reported. It is in compliance with this federal requirement that the social security number is important.

The mission of the consumer credit reporting industry is to provide accurate credit histories in the form of accurate consumer reports to credit granters to facilitate consumer transactions. This service fuels the U.S. economy and makes it possible for your constituents to buy homes, cars, and other goods and services with relative speed and ease. No other country has a comparable system.

Consumers, in the interest of obtaining credit, are very anxious that lenders see their entire credit history. Credit granters, in the interest of making the sale and receiving payment, depend on the credit reporting industry to provide them with fast, accurate information on which to make a credit decision. Today's credit reporting systems are designed to serve both needs.

The social security number enhances the credit bureau's ability to provide a complete and accurate credit history file on the consumer to the credit granter. It is used to merge fragmented files, to prevent the merging of wrong information into one file and to locate files that could not otherwise be retrieved based on names and address.

The credit bureau obtains the consumer's social security number in three ways. First, if a credit granter making an inquiry about a consumer includes the number in the inquiry process, it is captured by the credit bureau if it is not already an element in file. A very high percentage of inquiries include the consumer's social security number. Second, credit granters contribute their customer credit history to the consumer reporting agencies each month by automated tape and if the social security number is recorded, the credit bureau captures the number for the consumer's file. The third method is when consumers provide the number voluntarily to the credit bureau.

Credit bureau file structure is primarily based on name and address, but other identifying elements of information are used including social security number, former address, date of birth and generation code (Jr. - Sr.). The full credit report is not accessible to subscribers who inquire with only the social security number.

As we have all experienced at one time or another, our name or address is often given in different or varying ways. It is rarely a unique and consistent identifier, even though it refers to one person. Perhaps a simple but real example will bring my point out more clearly.

My birth certificate identifies me as David Barry Connelly. In preparation for this testimony I reviewed various accounts and other important documents to prove my point. I found that I am variously known to my creditors as:

D. Barry Connelly
D.B. Connelly
Barry Connelly
Barry D. Connelly

The U.S. Army and my AARP membership insist that I am David Connelly. In addition, I have given up trying to correct those who insist on spelling my first name with an "E" or my last name with an "A" or a variety of other phonetically correct Irish pronunciations.

Combine the lack of consistent name identification with creative descriptions of my 10907 Glenway address in Houston and the fact that I am moving in July to the Washington, D.C. suburbs, and it is easy to see that use of my social security number will enhance the accuracy of my credit record.

The use by credit bureaus of the social security number compensates to a very great extent for the inconsistent, inaccurate and non-unique use of name and address identifiers because it enables the credit bureau to find more of the consumer's credit history and enables the bureau to distinguish between consumers who have or use similar or identical names and addresses. We caution, however, that the social security number is not a panacea for accuracy, but inability to use the social security number as an identifier would only result in lessening the ability of the consumer reporting industry to meet the Congressional mandate in the FCRA to follow reasonable procedures to assure maximum possible accuracy of the information reported. ACB believes that consumers and credit granters would suffer the consequences of less accurate and complete information being available.

The credit reporting industry does provide a valuable locator service to those who have had a relationship with the consumer but have lost contact. The credit bureau will provide a new address on an individual if given the social security number, for such purposes as collection of outstanding debts, child support payments or delinquent students loans. Credit bureaus do not sell lists of social security numbers.

Importantly, the Fair Credit Reporting Act limits access to the information in our member files only to those with a permissible purpose as defined by law. Credit bureaus are required to obtain certification from users that the information will only be used for a lawful purpose and that is usually done by signed contract. An individual must lie and consciously violate the FCRA to obtain information without a permissible purpose. The violation is punishable by a $5,000 fine and/or one year in prison. A person may at the same time be in violation of the Computer Fraud and Abuse Act of 1984.

In recent testimony before another subcommittee of this House, ACB members recommended that Congress increase the penalties for violation of the FCRA to a felony and further recommended that individual consumers whose files were impermissibly accessed be allowed to bring civil action against the person violating their privacy.

In conclusion, the members of Associated Credit Bureaus are attempting to achieve the delicate balance between a Congressional mandate to report with maximum possible accuracy and the legitimate concern we all share over unwarranted invasion of personal privacy. We desire only to be good corporate citizens who provide an indispensable service to the economic health of the country. We do not seek to be a part of "one large information network." We believe our use of the social security number as described, provides more benefit than any perceived threat to American consumers.

Thank you and I will attempt to answer your questions.

Chairman JACOBS. Thank you, Mr. Connelly.

Mr. McDermott.

[No response.]

Chairman JACOBS. Mr. Gibbons.

Mr. GIBBONS. Thank you, Mr. Chairman.

Mr. Rothfeder, and Mr. Connelly, we kind of come at this thing from different directions but I think that both of you come to the same fact that we do need some kind of identifying number because the number of names that we have that are so similar, is that correct?

Mr. CONNELLY. Yes, sir.

Mr. ROTHFEDER. Yes, sir.

I don't think that, I mean I agree with Mr. Connelly in the sense that they have got to assure accuracy and they have got a delicate balance in a way. I mean you want your credit report to be accurate and they always get yelled at when that's not done, and on the other hand, they have to be careful to protect people's privacy also.

So it started 20 years or so ago when they computerized that they started using that and no one stopped them then and I doubt that you could really tell them to repeal that way of doing business at this point.

Mr. GIBBONS. Tell me, how much trouble do you have with Social Security numbers, other than transpositions of the number?

Mr. CONNELLY. Well, sir, that is a very good question. Certainly people, my wife might give mine thinking that she is doing the right thing, being perfectly innocent in doing it. And that, of course, causes an identification problem. People just don't remember their Social Security number, they don't have it, they don't know what it is.

So then you are stuck with using the name identifier. The fact that we can't really verify and I understand and have listened to the testimony, but I have to tell you that the fact is that we can't verify is obviously—it is not a verifiable number. So that causes a problem.

Mr. ROTHFEDER. I think the reason why I brought up the issue that somebody has got to be held responsible a little bit further down the chain is that in my investigations frequently people will, on their credit reports, will have two or three names attached to the same Social Security number because a lot of people let their wives or even their secretary get credit cards in their names. They give them credit cards for convenience sake and then that Social Security number gets attached to someone else and sort of starts flying around the system in that way.

So, again, I think on the bank level or the person who is going to give out loans or whatever, they should look further into it, and should say, who is this person I am giving out a loan to before doing it.

Mr. GIBBONS. Do you think we are going to come eventually to a national card system of some sort?

Mr. CONNELLY. Well, Mr. Gibbons, that you said it right earlier, it is de facto that it has become a number that we all use. Whether or not you identify it as a card system, sir, I think that's a judgment call for Congress, but we need an identifier.

Mr. **Rothfeder**. Yes, I think that for data banks that have to keep their accuracy in check they need that kind of information. I would oppose a national identifier, meaning every person is stamped with a particular number that travels through life with them. I would rather that the corporations deal with their own problems and if they are using Social Security number so be it, but that is their numbering system.

Mr. **Gibbons**. I know from keeping up campaign records. We have a terrible time keeping track of people, particularly ladies, changing their names in marriage or divorce or something like that.

How do you handle all of that?

Mr. **Connelly**. Yes, sir, it is because of the Social Security number that you give a good example. In a campaign situation where you have a name change or you don't want to misidentify someone when you send out a Dear Barry and Phyllis letter, you don't want to do it wrong. That is maybe not quite as serious as a credit history, but we likewise, don't want to do it wrong.

In a female situation, like you are talking about with ladies, when they get married because of the Social Security number, we can better allow her to be able to use her previous credit history by being able to obtain it because we have her Social Security number prior to her marriage. So that we are not just relying on the name. That's how we use it, that's how it helps the system, Mr. Gibbons.

Mr. **Gibbons**. Thank you.

Chairman **Jacobs**. Mr. Wiggins, were you falsely charged with a crime as a consequence of the misuse of the Social Security number?

Mr. **Wiggins**. Like I said, it added authenticity. Anyone who would look at that report said to me, well, isn't this your Social Security number? And I said, yes, it is, but that did not make me that person.

Chairman **Jacobs**. Yes, I understand that but I did not quite understand your testimony. You were never actually charged in consequence of the misidentity? It was just that you were identified as a person who had been charged with a crime, is that it?

Mr. **Wiggins**. Right, through the Social Security number and I have lost my employment and the whole war story.

Chairman **Jacobs**. Good. Well, Mr. Crane.

Mr. **Crane**. Thank you, Mr. Chairman.

Mr. Connelly commented that nobody knows his Social Security number. The amazing thing I have discovered is that my kids can rattle theirs off that fast. I can give you my serial number from when I was in the Army and that goes back about 30 years. If it were not for my driver's license I could not tell you my Social Security number. It is on the license.

Chairman **Jacobs**. Can you give your rifle number?

Mr. **Crane**. No, I can't give you my rifle number, Andy. [Laughter.]

But frankly, when I was in the teaching profession down at Bradley University, I had a colleague who was a refugee from Hungary. When the Nazis took over Hungary although he was not Jewish he provided sanctuary and hid Jews out. He pointed out the tattooed numbers on everybody's arm. And he freaked out when they talked about issuing Social Security cards to little infants.

And he said, why don't they just put the tatoo on everybody's arm? There is precedent for this. I confess I find it troublesome. I was told—I don't know whether this is accurate or not—but I was told that not too many years ago you could walk into any cemetery in Chicago and find a name on one of the tombstones in which the age was roughly your own and write to the Social Security Administration and tell them that you lost your card and they would send you a new card. Their records were so incomplete that they did not know whether the person was dead or not.

I would assume that if, in fact, that were true that they have tightened up considerably because of illegal aliens in the country. But, with that Social Security card and with the opportunity to contact Cook County bureaucrats, you can tell them that you lost your birth certificate, then apply for a driver's license and you are home free.

It seems to me that is a process that, when you have got 250 million people, creates a potential for all kinds of abuses. The ones that Mr. Rothfeder cited in his testimony are illustrative of that.

I thank you for your input. I don't really have any significant questions, but I am disturbed about the entire issue.

Chairman Jacobs. Well, we thank you, very much, for your contribution to the record.

Our next panel consist of Ms. Baskin, Dr. Culnan, and Mr. Hendricks.

STATEMENT OF ROBERTA BASKIN, CONSUMER EDITOR, WJLA-TV, WASHINGTON, D.C.

Ms. Baskin. I will go ahead and start. Good morning, my name is Roberta Baskin and since 1984, I have been the consumer investigative reporter at WJLA, Channel 7, here in Washington.

Last November, I presented a series of reports called "Privacy For Sale." It looked at how easily personal information about us is gathered, disseminated and sold without our knowing it and without our ability to stop it. The committee suggested a little show-and-tell to support my testimony so I am going to do the show part first, if I can. And it is the part of my series focusing on credit agencies, credit bureaus and the ease with which they can obtain our financial records.

[Videotape shown.]

Ms. Baskin. Not all of our stories have happy endings like that. During the course of our investigation I became increasingly amazed just how tuned in credit bureaus are to our financial records, and how sophisticated their marketing techniques are. They know our annual income, they know how we spend it, and more and more records of our credit card transactions end up in computer files of the big three credit bureaus: TRW, Trans Union, and Equifax.

The information is broken down and categorized according to marital status, address, age group, neighborhood, family size, income level, spending habits. From there, the information is sold to marketers who use that information to construct consumer profiles so that they can narrowly target their marketing campaigns.

If you ever wondered how you got on the mailing list of so many junk mail distributors, it is a result of your spending habits. Your name has been categorized and probably can be found in dozens of marketing lists. Trying to get your name off those lists is nearly impossible.

There is little you can do to keep your name from getting on those lists in the first place. One woman that I interviewed in my series, a doctor, had merely inquired about a dating service called Jewish Introductions International and she was told that information about her would be kept strictly confidential. I am the one that finally told her that personal information about her was sold on a list that included upscale singles with incomes of over $50,000, and, in fact, the dating service literally sold her name on mailing labels. I brought the list here. These are all the mailing labels that they send out for a price. The woman was insulted. She said that two of the most private aspects of her life—her religion and her marital status was breached for a price. I paid $265 for the list, and it includes the names of hundreds of District residents. None of the residents that we contacted knew that their names and information about them had a price tag on it.

Who else is in the business of selling your name on a mailing list? Well, the Department of Motor Vehicles in the District, Virginia, and Maryland; and some 30 States also collect Social Security numbers as part of their data bases; the Postal Service sells change of address information now; and at least one U.S. Senator, that I know of, sells the names of letter writing constituents to conservative causes.

As you saw on the tape, I checked into my own credit records and found that there have been 15 outside inquiries into my financial status and my spending patterns. I also found that some of the information contained in my credit cards was wrong, particularly the wrong Social Security number and I tried twice to change it over the phone, to correct the information. I was told that I have to do it in writing. The credit bureau does supply forms that you can fill out to challenge the information that they got wrong, but as you saw in my report that is not a fail-safe procedure so that I have yet to get that done.

During my investigation, I also contacted a private detective who could do most of his leg work without ever leaving his home computer. So I simply gave him my name, that's all. Within minutes he was able to call up my married name, my unlisted phone number, my current and some prior addresses, the names and phone numbers of five of my neighbors and five previous neighbors in Chicago, my birth date, and my Social Security number.

I found that it really wasn't his skill that enabled him to obtain that information; it was the software and anyone who owns a computer and a phone modem can get into it and get access to it.

I conducted a little privacy survey of my own on the corner of Connecticut Avenue and M Street, here in the District. Most of the passers-by that we interviewed said that they valued their privacy and they would never give out their Social Security number unless it was required. Then we set up a little table with some ice cream and a marketing survey and we asked them to list their personal information, including their Social Security number on a marketing survey form in exchange for an ice cream and here is the survey: 23 out 25 of the people put down their Social Security number.

People believe that that kind of information can't go anywhere without their approval. They believe that their privacy is protected. But I came away from this investigation understanding that the consumer, private citizen is virtually unprotected from outside inquiries. The one law that has been passed in the last several years is the Video Privacy Protection Act, the so-called Bork bill, which was passed after an enterprising reporter got access to the kinds of movies that Judge Bork was renting.

As you consider legislation that would permit using Social Security number to better keep track of people, please consider that private interests are already doing that. Access to our personal information and the advanced technology that is used to spread it is already decades ahead of the laws written to protect us.

Thank you.

Chairman JACOBS. Thank you, Ms. Baskin.

Dr. Culnan.

STATEMENT OF MARY J. CULNAN, PH.D., ASSOCIATE PROFESSOR, SCHOOL OF BUSINESS ADMINISTRATION, GEORGETOWN UNIVERSITY, WASHINGTON, D.C.

Ms. CULNAN. Thank you.

My name is Mary Culnan and I am on the faculty of the school of business administration at Georgetown University where I teach information systems. I thank you for inviting me to come and testify before you today.

As you have already heard, the private sector makes widespread use of the Social Security number. I oppose this practice except where it is required by law for the reasons that have been cited by all the previous witnesses.

In 1974, the Wall Street Journal lamented the fact that this phenomenon of the widespread private use of the Social Security number would cause our Social Security numbers to become the "red flag of misery" and, in fact, I think this is happening for a lot of people.

Earlier this year, the Wall Street Journal published what is probably the most stunning example of private sector misuse of the Social Security number when it described Fidelity Investments customer service information system where you picked up a touch-tone phone and dialed the 800-number and punched in the Social Security number of any Fidelity investor and, were read back by the computer voice at the end, a complete summary of that person's investment portfolio. There was no PIN number required, no security code, and, because Social Security numbers are so widely available—for example, if a Member of Congress releases his or her tax records, anybody that has that information, in fact, has access to the Social Security number and can call up and find out what is really considered to be private information, I think, by all of us.

There are many more mundane examples closer to home. I collected some examples and brought these with me. At my own university, right on my ID card, there is the Social Security number and that is how I am identified. And that is how all of our students are identified with the Social Security number despite the fact that there is also a number on the card which is also unique.

Credit cards. If you want to apply for a credit card, you are always asked to give your Social Security number. If you are a student establishing credit, you are asked to supply your student ID number or a transcript and, there goes your Social Security number.

Also, if you want to get check cashing privileges at the Giant grocery store, they ask for your Social Security number, they ask for your driver's license which, in the District of Columbia, is my Social Security number. If you want to rent videos at Erol's they ask for your driver's license number and that is my Social Security number.

At American University, where I also have library borrowing privileges, they will not let me check out a book without providing my Social Security number. When in fact, there is another number that they have that I provided to them that is unique that they could use instead.

But a lot of this, I think is organizational inertia. At Georgetown, if I want the library to recall a book and send me a postcard saying the book is back in the library I have to give them my Social Security number again, even though there is a number on the back that is my actual library borrower number.

So the list goes on and on. I think the bottom line, as Mr. Gibbons said also, is that people should not have to drop out of the economy to maintain their privacy and this is one of the issues that is at hand.

I would like to conclude by making three recommendations which I hope the committee will consider. First I think there ought to be some legislation introduced to really put some clamps on the private sector use of the Social Security number. The main reason for doing this—I don't believe that legislation is the panacea for all of society's ills, but I do believe that the hearings that would be associated with such a bill would really bring everybody to the table and start the discussion. And that is what we need, to have some discussion among the public that are concerned—consumers, privacy advocates, business, the credit bureau people and all the rest.

Second, before any regulation is enacted, if it should be, that regulates or affects current practices, we really need what I call an "information systems impact assessment" like an environmental impact study. That to document the state of the current practices in the private sector. We really don't know this nor do we know what the impact would be if, in fact, laws were written to change things that people have been doing for 25 or 30 years and in which they have a major investment.

Therefore, I recommend that the General Accounting Office be asked to do a survey, to go out and document the extent of Social Security number use, not only among private or single firms in particular industries, but also where there are electronic linkages across industries and across firms. I think the credit industry is a really good example of how complicated information use has become. There would be a real benefit in taking a look at this.

Finally, I think we need to send a message that, in fact, our Social Security numbers are not up for grabs. One way to do this would be to establish a clearing house either in the Social Security Administration or with a data protection board, if such a board is established. There is legislation pending on this. And if you, as a private organization, were going to establish a new use for the Social Security number, you would be required to file notice with the clearing house and accept public comment. This is not a proposal for data registration, just to send the message to companies that they need to think about what they are doing and if the public objects, there are perhaps proposals that would be withdrawn voluntarily.

In conclusion, I think addressing these privacy concerns in a way that balances everybody's interests—that of business, consumers, privacy advocates and other stakeholders—will require both creativity and patience and I hope that we will bring these to the discussion.

I thank you for the opportunity to present my views, and I would be happy to answer any questions.

[The prepared statement follows:]

TESTIMONY OF MARY J. CULNAN, GEORGETOWN UNIVERSITY

Mr. Chairman and members of the Subcommittee, thank you for inviting me to testify at this hearing on the use of the social security number as a national identifier. My name is Mary Culnan and I am an Associate Professor in the School of Business Administration at Georgetown University. I have been a computer professional since 1968. Prior to earning my doctorate in business administration, I was employed as a systems analyst by a Fortune 500 company for eight years where I developed database applications for my employer. Since 1980, I have been a professor of management information systems. For the past eighteen months I have been conducting research on consumer privacy. During the last session of Congress, I co-authored statements for hearings on privacy conducted by two different House of Representatives Subcommittees.

I am pleased to testify about the issues that are raised by private sector use of the social security number. Today we revisit many of the same issues which were raised when Congress debated legislation that resulted in the Privacy Act of 1974[1]. A Wall Street Journal article published just prior to passage of this legislation lamented the fact restrictions on private sector use of the social security number had been deleted from the legislation, raising the potential for the social security number to become "a red flag of misery."[2]

Nothing illustrates this point better today than a recent Wall Street Journal story about Fidelity Investments' customer inquiry system.[3] By calling a toll-free number and entering their social security number using a touchtone telephone, callers were provided an audio summary of their Fidelity holdings. Because the system did not require the caller to enter a PIN number, anyone knowing the social security number of any Fidelity customer could gain access to information about that individual's account. Because social security numbers appear in so many places including the front of some checks, on drivers licenses, in documents filed with the SEC and even on tax forms made public by elected officials, the system created an enormous potential for widespread violation of the privacy rights of Fidelity customers.

My position is that individuals should not be denied the opportunity to participate in our economy because they object to providing their social security number when its use is not mandated by law.[4] I personally oppose the use of the social security number by private sector organizations except as required by law. However, I also recognize that prohibiting the use of social security number today would present tremendous implementation problems for a large number of organizations which have an enormous financial investment in their existing information systems.

Private firms use the social security number as an identifier because it facilitates their record-keeping. One of the early factors which motivated organizations to acquire computers was the need to process records more efficiently--faster, with fewer errors, and at lower costs. Today it would be unusual to find even a small business that did not keep its customer records on a computer. However, as everyone in this room knows first-hand, errors do occur. Companies fail to record our payments correctly, or we are billed for someone else's charges, etc. To minimize the probability of these transaction processing errors, a company will assign a unique, usually numeric, identifier to each of its customers [and employees]. Payments, purchases, deposits, withdrawals, overtime hours, retirement contributions, subscription renewals, etc. are posted to the correct customer master record in the database by matching the identifier on the transaction with the identifier in the master record. The same identifier is also used to access an individual's account in order to respond to inquiries, such as using an ATM machine to check the current balance in your checking account. Here, the identifier is read from the magnetic strip on the ATM card.

---

[1] Legislative History of the Privacy Act of 1974, S.3418 (Public Law 93-579). Committee on Government Operations, United States Senate and Committee on Government Operations, House of Representatives, 1976.

[2] Arlen J. Large, "The Continuing Problem of Privacy," Wall Street Journal, November 13, 1974 (reprinted in the Legislative History of the Privacy Act of 1974, p. 1237-1239).

[3] Clements, Jonathan. "Finding Out How Your Neighbor Invests in a Free Phone Call Away." The Wall Street Journal, February 4, 1991, page C1.

[4] This provision was included as Sec. 203 in the original version of the Privacy Act of 1974 (S. 3418) introduced by Senator Ervin on May 1, 1974.

Today, the widespread use of relational database technology makes it possible to access any given record in a database using either the identifier, or many other fields in that record. For example, an individual's record might be retrieved by using the individual's name, telephone number, or date of birth as well as the unique identifier assigned to that record. However, these other fields are either not unique (name, date of birth), are unique but subject to change (telephone number), or do not meet other tests for a standard identifier. As a result, organizations still use an identifier, or key, to ensure that a single record in their database can be retrieved unambiguously.[5] This key, is used to break ties when other fields such as name are also used to retrieve a record, and to allow record processing to be performed efficiently when the key is used alone[6].

As this Subcommittee is already well-aware, the social security number is widely-used as an identifier by the private sector[7]. For example, my own university uses the social security number as its employee number as well as the student identification number. Applications for credit cards and check-cashing privileges routinely ask the applicant to supply their social security number. Individuals who wished to "opt out" of the Lotus MarketPlace[8] were asked to supply their social security numbers in addition to their names and addresses, suggesting that the source data were keyed on the social security number[9]. In my opinion, this widespread use by the private sector of an identifier that was intended only for use by the Federal Government is the source of two problems.

---

[5] The criteria for a Standard Universal Identifier (SUI) include uniqueness, permanence, ubiquity, availability, indispensability, brevity and reliability according to the Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, U.S. Department of Health Education and Welfare, 1973, pp. 109-111.

[6] For a detailed discussion of the role of the key in relational database systems, see David M. Kroenke and Kathleen A. Dolan, Database Processing: Fundamentals, Design, Implementation, 3rd edition, Chicago: Science Research Associates, Inc., 1988, pp. 139-141.

[7] See for example Robert Ellis Smith, Report on the Collection and Use of Social Security Numbers, Privacy Journal, 1990.

[8] The Lotus MarketPlace was a CD-ROM database of personal information on 120 million Americans which was based on summarized credit report data provided by Equifax. Lotus Development Corporation and Equifax, Inc. jointly withdrew the product on January 23, 1991 in the wake of consumer protests.

[9] There is no reason to think that Lotus planned to distribute social security numbers as part of the Lotus MarketPlace product. It is likely that instead, the social security number was used internally within Lotus and Equifax (the data supplier) to key the

First, when any common identifier is used by many organizations, it increases the probability that information from disparate sources will be combined. Today, we are seeing a growth in inter-organizational information systems -- direct electronic links between computers of two or more companies. By eliminating paper transfers of information and the associated handling costs and delays, these electronic linkages allow American firms to be more competitive. However, when records move across organizational boundaries, any errors contained in those records also travel.

There is some evidence that the widespread use of the social security number leads to widespread errors in large record-keeping systems. In my opinion, this is because of the special role the social security number plays as an identifier for the Federal Government, most notably the Internal Revenue Service. For example, in 1982, banks in Massachusetts were asked by the state to run a match on social security numbers in order to identify "welfare cheaters." The twenty-three participating banks reported a 30% error rate. Some of the errors were the result of data entry errors or other legitimate errors, but a substantial proportion of the errors were the result of customers who reported false social security numbers to avoid Federal taxes.[10] Matching projects were also sponsored by the Social Security Administration between 1984 and 1988. Matches performed by Citicorp and by TRW resulted in error rates due to incorrect or unverified numbers of 46% and 28% respectively.[11]

The second problem stems from the fact that by using the social security number, the private sector and the public sector have adopted a common identifier. The use of any common identifier such as a telephone number by many organizations facilitates the compilation of dossiers and therefore presents a threat to individual privacy, However, I believe that the use of the social security number by the private sector poses an unusual threat to privacy as it creates a strong temptation to develop programs to match public and private sector records. Thus, the concerns raised by the framers of the Privacy Act of 1974 are still valid today.

There are a number of actions that Congress could take to address the issues raised by the widespread use of the social security number by the private sector. First, legislation could be introduced banning the use of the social security number as an identifier by the private sector except as required by law. An alternative proposal would be to reintroduce the 1974 proposal which would make it illegal to deny benefits to any individuals who declined to provide their social security number when the number is not required by law[12]. Hearings on these bills would clearly

---

database.

[10] "First Bay State Bank (A) & (B)," (case study), Harvard Business School 9-186-042, 9-186-042, 1985.

[11] Evan Hendricks et. al., Your Right to Privacy: A Basic Guide to Legal Rights in an Information Society, 2nd ed., Southern Illinois University Press, 1990, p. 66.

[12] "It shall be unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or enter into any other business transaction or commercial relationship with an individual (except to the extent specifically necessary for the conduct of administration of the old-age, survivors, and disability insurance program established under title II of the Social Security Act) in whole or in part

start the discussion and bring parties from the affected industries to the table, even if these bills have only a small chance of being enacted, or if enacted, the law would be difficult to enforce[13].

Second, we clearly do not have a thorough understanding of the extent of private sector use of the social security number. It would be useful to have the General Accounting Office conduct a study to document not only the extent of use by single firms in various industries, but also the extent to which inter-organizational systems are linked by the social security number. In particular, the study should document these issues in the credit industry, and should focus on the information requirements of the credit grantor-credit reporting agency relationship. I believe such an "information systems impact assessment" is an essential prerequisite to enacting legislation that would regulate current practices.

Finally, the Social Security Administration could establish a clearinghouse on new private sector uses of the social security number. All private sector organizations which intend to develop new applications where an individual is asked to supply their social security number for reasons not required by law would be required to file a notice for public comment with the clearinghouse in advance of actual implementation of the application. Public comment could be solicited both in writing or electronically using the public computer networks such as Prodigy, the Well or CompuServe.[14]. It should be noted that this is not a proposal for a data registration system; here private sector organizations would **not** be required to gain a license for use of the social security number as is the case in some European countries[15].

In conclusion, today we have seen that many of the privacy concerns raised by Congress in 1974 persist today, while new technology applications continue to raise new concerns. Addressing these issues in a way that balances the interests of business, consumers, privacy advocates and other stakeholders will require both creativity and patience. I hope this hearing represents the first step toward such an outcome. Thank you again for allowing me to present my views to the Subcommittee.

---

because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by law," Sec. 203 of S. 3418, May 1, 1974, Legislative History of the Privacy Act of 1974, p. 23-24.

[13] In Where the Law Ends: The Social Control of Corporate Behavior (Harper & Row, 1975), Christopher Stone discusses the problems of controlling corporate behavior through economic sanctions imposed by law.

[14] Instead of the Social Security Administration, responsibility for the clearinghouse could be assigned to a Data Protection Board. If enacted, HR 685 will establish such a board in the United States.

[15] See David H. Flaherty, Protecting privacy in Surveillance Societies, University of North Carolina Press, 1989, for information about European data protection laws.

Chairman Jacobs. Thank you, Dr. Culnan.

Mr. Hendricks.

STATEMENT OF EVAN HENDRICKS, PUBLISHER AND EDITOR, PRIVACY TIMES

Mr. Hendricks. Yes, I am Evan Hendricks and editor and publisher of the Privacy Times newsletter and I thank you, very much, for the opportunity to testify here today.

I think it is an important hearing to focus on the Social Security number because I think that what has happened to the Social Security number is very symbolic and representative of what has happened to our privacy: It has been a slow and gradual erosion. The Social Security number, as Congressman Pickle so ably pointed out, had an original purpose for keeping wage records. Then it became a slow march where it became an identifier for the IRS and then all Federal agencies, and then driver's licenses. And now banks are required under the law to use this for the matching process with the IRS.

So it has been a slow march. In the same way our privacy has been gradually eroded by easy availability of personal information, and the technology's ability to manipulate it and draw out profiles on us.

One significant aspect about the Social Security number, is that it allows for the interconnection of data bases. It allows for the computers to talk to each other and to search through each other's records and find common people in different data bases. That allows you, much like bar hopping, to go data base hopping, as you search for people and their characteristics.

We used to worry about Big Brother—the one big Government centralized data base. But with technology and with the Social Security number as a unique identifier, we really have to worry about Little Brother now, going back to the interconnection of all of these data bases.

In the context, I think we have a situation where we have old, out-dated privacy laws which are badly in need of updating and Congress is going to be examining some of these; and we have very loose practices throughout big institutions—Government and the private sector. I call this the cowboy atmosphere.

An example of this is something that the subcommittee is very familiar with—the match that the Social Security Administration was secretly doing with TRW and Citibank to verify Social Security numbers. One of the things that did not really come out too visibly in that was that both for the Citicorp files and for TRW, there was a 30 percent inaccuracy rate among somebody's Social Security numbers; presumably Citicorp's or TRW's, which is why they wanted to do the match in the first place. So I think using the Social Security number does give us a false sense of security and that the TRW-Citibank-SSA match is very good evidence of that.

In a cowboy atmosphere if, like Professor Culnan was describing, if you want to protect your privacy, you sometimes must take things in your own hands and become a Jesse James six-shooter. I got a call from a man in New Jersey named Don Pensa, who feels strongly about not giving out his Social Security number because he remembers the original pledge that this number is not for identification and he wants to try and make people stick to that. He is a New Jersey resident and the New Jersey DMV was switching over to a Social Security number and he got into a big phone fight with them. He said the whole place came to a standstill when he insisted that he could go on without giving his Social Security number. But he finally won that one. He did the same thing with the Federal Aviation Administration for his pilots license.

Then the fuel oil company said that they could not make him a customer, they would not sell him fuel unless he gave them a Social Security number. He told them he would go somewhere else. They put him on hold, then came back and said, "OK, we will sell you fuel without getting your Social Security number." But he has not had that kind of luck with health insurance. He has not found a health insurer who would give him insurance without giving his Social Security number. That's how serious the issue can be sometimes.

I would like to quickly mention that one thing I have seen, over the years, is that bad policies or badly managed programs often lead to a privacy invasive solution or approach. I think that the immigration issue and computer matching are good examples. Computer matching, which relies on the Social Security number has not been proven to fight fraud or save the Government money. Government agencies have not even come up with a methodology to account for how the costs and the benefits shake out.

In the same way, I think that the fact that they are proposing this eligibility card—and this view is spelled out in more detail in my testimony—shows there is something more fundamentally wrong with our immigration policy. I refer you to my testimony on this point, but I think it is something to watch out for, when you get to the point where you want these national identifier numbers and these other things that turn us into a great Big Brother system, they are trying to save programs that should be going in the other direction.

It is a bleak picture in some ways but there are very simple solutions to these problems. The subcommittee hearing is a very good start because you have jurisdiction over the number and you will be able to take a hard look at what is going to be happening with it.

Second, I think that like Professor Culnan, I endorse her view that we need to have a better understanding of how this is used and not just GAO but maybe the Office of Technology Assessment would be a good place to start to really give us the information we need to what is the fullest extent of the use and what are its implications for privacy?

I agree with Congressman Pickle's view that maybe we should have a moratorium on new uses of the Social Security number in the private sector. I would like to emphasize how important it is that we, like other countries, adopt or create some sort of data protection board. For example, the Canadian Social Security number is called the Social Insurance number, or appropriately, the SIN number. The Canadian privacy commissioner recommended that the government curtail use of the SIN. He did a study, like one we are talking about here, and said the SIN was not necessary in certain ways. The government said, fine, and they actually rolled back the use of the number.

So I would like to emphasize that Congressman Wise's bill is a good vehicle for discussion on this kind of approach and in relation to the number, as well as other issues, it can play a very helpful role for Congress, the media and as we approach the privacy issue in the 1990s.

Thank you.

[The prepared statement follows:]

TESTIMONY OF EVAN HENDRICKS
PRIVACY TIMES

Mr. Chairman, I'd like to thank you for this opportunity to testify before the subcommittee and express my appreciation for the hard work you and your staff have put into to this historic effort to focus attention on uses of Social Security numbers and related privacy issues.

My name is Evan Hendricks. I'm editor/publisher of PRIVACY TIMES, a biweekly, Washington-based newsletter that reports on legal, policy, industry and consumer news in the fields of privacy and freedom of information. I started PRIVACY TIMES ten years ago. I have been reporting on privacy and FOIA issues for 13 years. I am author of the book Your Right To Privacy (SIUP-1990).

We are at a stage of history where our rights to individual privacy are seriously threatened. There are many reasons. First, there is the growing use of the Social Security number as a universal identifier. Second, advances in information technology allows for faster and easier gathering, sharing and manipulation of personal data. Third, there is easy access to volumes of personal data from both public and private sources. Finally, privacy laws, where they exist, are out of date and badly in need of strengthening. For some kinds of personal information, there are no controls.

These and other factors have created what I describe as a "Cowboy Atmosphere," in which large institutions and small entrepeneurs alike feel free to use, and as some see it, abuse personal data with little regard for the individual's concern for privacy.

There are legislative solutions to many of the privacy problems facing us. But they require Congress to move on several fronts and to engage in the challenging process of enacting laws which strike the proper balance. I hope that these hearings will lead to new proposals to control the SSN, and that other Congressional panels will follow your lead in areas over which they have jurisdiction.

Background

Why is it so important that Congress act? Mainly because the Supreme Court ruled 15 years ago, and consistently held ever since, that under the Constitution, we have no right to information privacy.

Although the Founding Fathers intended that we "be secure in our personal papers," the Burger Court reasoned that when we open a bank account, we voluntarily surrender information about ourselves to the bank. The information then becomes part of the "flow of commerce," and belongs to the bank, not to us. Under the Constitution, the Court ruled, there is no protection for personal information held by third parties. Absent statutory restrictions, the banks therefore were free to give our personal data to anyone they pleased. The message from the Supreme Court was clear: if you want privacy, take your cash home and stick it under the mattress.

The Supreme Court has extended this reasoning to telephone and other third party records. In 1989, the Supreme Court even ruled that we had no constitutional expectation of privacy in our garbage, holding that once put out for collection, our garbage was available to everyone.

Of course none of these decisions were unanimous. Of the garbage ruling, Justice Brennan said the fact that burglars might enter private homes did not negate the right to privacy there. "Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior. I suspect therefore that members of our society will be shocked to learn that the Court, the ultimate guarantor of liberty, deems unreasonable our expectation that the aspects of our private lives that are concealed safely in a trash bag will not become public."

Congress has responded to some of these rulings, enacting statutes that provide differing protections for financial records, telephone records, video store rental data and cable television files. It's not my purpose here to give an overview of U.S. privacy law. Suffice to say that the current state of U.S. privacy law is a patchwork quilt sorely needing attention.

In my 13 years of following the issue, there have been consistent signs confirming that Americans feel strongly about their right to privacy and want stronger legal protections. This has been documented in three separate Lou Harris opinion surveys, the most recent being released last year.

What I have found dramatic is the past year's explosion in media attention to the issue, and the subsequent strong public response to that media coverage. Press attention to the uses and abuses of personal data have increased 20-fold, signifying that privacy is emerging as one of the key issues of 1990s. Response to news articles, documentaries and talk shows demonstrates that public is both anxious and angry about the way their personal data are used without notice and consent.

The 1980s' climate for handling personal data virtually dictated that privacy would become a major concern in the 1990s. In the beginning of the 1980s the Reagan Administration completely turned its back on seven years of bipartisan work by the Ford and Carter Administrations, a federal study commission and Congress to forge a national privacy policy. The Reagan Administration's decision to halt all work on privacy proposals sent a signal to government bureaucrats and certain industries that they could exploit personal data with little or no consideration for individuals' feelings about personal privacy. The 1980's free and easy use of personal data created its own backlash.

Moreover, the climate in Washington has improved because Dr. Bonnie Guiton, the President's Advisor on Consumer Affairs, for the past two years had made privacy a priority consumer issue. Dr. Guiton became the Bush Administration's de facto "point person" for privacy. She raised the visibility of the issue by organizing a national consumer conference on privacy, by testifying in favor of Fair Credit Reporting Act Amendments, and by creating various task forces and urging industry compliance with voluntary standards. Now that Dr. Guiton is joining Governor Wilson's Cabinet in California, many of us in the privacy community are hopeful that her replacement, Ann Wallace, will continue her work.

While the efforts of the U.S. Office of Consumer Affairs have been welcome, its jurisdiction is limited. Meanwhile, the Bush Administration has failed to move on several fronts to improve privacy policy as well as the federal government's own information practices.

SSN: A Case Study in Erosion of Privacy

The Social Security Card used to state: "This card is not to be used for identification." The promises in the early days that the Social Security number would not become an identification number has turned out to be one of the great lies to the American people, on par with other famous promises like "Your check is in the mail."

Clearly, the history of the Social Security Number (SSN) is a classic case study in the erosion of privacy. The SSN has proved to be the valuable key element that allows computers to talk to eachother, to search through eachother's data files and to draw out individual profiles on people. Accordingly, the creation of one, centralized computer system on all Americans is no longer the only privacy concern. Now the interconnection of small computer networks, made easier by widespread use of the Social Security number, is creating an enormous system capable of data surveillance.

The original use of the SSN, of course was to number personal accounts for the collection of taxes and benefits in the Social Security program. The first numbers were assigned in 1936. A year later, it was decided that the same identifier should be used to number accounts in state unemployment-insurance systems. In 1943, Executive Order 9397 was issued by President Roosevelt authorizing any federal agency to use the SSN for new data systems requiring permanent account numbers on records pertaining to individuals. This authority was not used for many years, even by the U.S. Civil Service Commission, for whose benefit it was originally intended.

In 1961, the Internal Revenue Service decided to designate the SSN as the taxpayer identification number. Thereafter, new uses followed in rapid succession: for Treasury Bonds, for old-age-assistance benefits accounts, for state and federal civil-service employee records, for Veterans Administration hospital records, Indian Health Service patient records, and as the military-

P ersonnel service number.

Congress also encouraged this trend. Under the Tax Reform Act of 1976, it authorized states to use the SSN for motor vehicle registration records and driver's licenses. Currently some three dozen states use the SSN as a driver identification number. As you know, this means that the number often is recorded on checks as an ID number when consumers made purchases. The 1976 law also authorized SSN use for administration of of local and state tax laws and of general public assistance programs and for implementation of the Parent Locator System.

Another major step came in 1984, when the Deficit Reduction Act required all depositors to provide to financial institutions their SSNs to IRS computers could match the amount of interest reported by taxpayers with the amounts reported to the IRS by banks. The law also required recipients of federal benefits to provide social service agencies with their SSNs. The 1986 Tax Reform Act requires parents to show SSNs for children over the age of five who are claimed as dependents.

Despite claims that the SSN was not, or would not become, an personal identification number, it clearly has increasingly become one. Fortunately, though, it does not qualify as a "universal" identifier yet. In hindsight, it should be clear that large institutions with mammoth, computerized data systems will always prefer to seize a common identifying number. To waggle such a tempting tool as an SSN in front of a large government agency or corporation and expect them not to use it is unrealistic -- like trying to roll a lamb chop past a wolf! That's why strong restrictions on the use of the SSN must be adopted.

Bad Policies & Management Get Worse

In the years I've been following these issues, I noticed that poorly conceived policies and/or badly managed programs can lead to proposals that not only do not solve the problem identified, but set disastrous precedents for our national privacy policy. Two prominent examples are computer matching as a "solution" to "fraud and abuse" in welfare and other social programs; and a work elgibility card (secure identification) as the answer for "too much immigration" to the United States. Use of the Social Security number was a key part of these "non-solutions."

In the late 1970s and early 1980s, reports were spreading about rampant mismanagement, fraud and abuse in welfare and other government benefit programs. The solution favored by agency bureaucrats was to computer match different agency databases. For instance, a list of welfare recipients could be matched against a roster of federal employees to see if anyone was working and receiving welfare at the same time. The match was made possible by comparing SSNs in various databases. This practice appeared to violate the Privacy Act's prohibitions against disclosing personal data without the individuals' consent. Initially, some matching programs resulted in people being falsely branded cheaters, as well as other unnecessary disruptions in people's lives and government programs. Some federal bureaucrats maintained that computer matching saved millions of dollars. But a decade later, the General Accounting Office found that not only could agencies not prove that matching had saved any money, but that agencies had not even developed a reliable methodology for calculating costs and benefits. In a recent Health and Human Service Department report, the inspector general admitted that in California's best anti-fraud program, computer matching only identified 12 percent of the cases. The more effective approach, of course, involved hard work by cooperating case officers and investigators in identifying unusual patterns -- in other words, sound management appoach. In this supposed fight against government fraud and abuse and the misplaced reliance on computer matching, federal bureaucrats appeared to give little attention to improving their own management and oversight of these programs. Instead, the computer matching approach gave the appearance that something was being done without really getting the job done.

Meanwhile, computer matching set disastrous precedents for our national privacy policies. Other Western nations have studied U.S. computer matching programs and decided not to make the same mistakes by placing restrictions on the practice before it became widespread.

A central lesson to me was that the U.S. decision to go with the privacy invasive approach of computer matching was the unfortunate but logical result of exasperated decision-makers trying to show they were doing something about a badly mismanaged program.

I think the same analysis can be applied to the debate over immigration and the privacy invasive proposal involving the work eligibility card. This entire approach stems from a 1980 immigration reform commission that, for whatever reason, was out of touch with the realities of immigration to the United States, and the American people's strong and well-documented opposition to a national identity card.

The commission began its analysis by stating foreigners came to the United States for jobs. Therefore, to stop the flow of "illegal" immigration you had to make it illegal for for employers to hire undocumented workers. Of course, this proposal was problematic because it would cause employers to discriminate against foreign-looking or -sounding workers. So the next logical step would be to require all job applicants, regardless of race, creed or color, to show a work eligibility card or "secure" Social Security card. Congress eventually adopted the employer sanctions approach but rejected the work ID card, instead opting for job applicants showing existing forms of identification to prove they were here legally. Last year we saw that some in the so-called "immigration reform" movement hoped to bring their Work ID card proposal back to life through legislation that would have started "pilot projects." Fortunately, the proposal was defeated.

From what I've read, employer sanctions have not done much to discourage undocumented foreigners from seeking work in the United States. Again, I think the fact that "immigration reformers" concluded that a national identity card was the answer in fact showed that there was something more fundamentally wrong with our immigration policy and management of our immigration programs. I believe history has shown that people migrate to this country when life in their native country, either economically or politically or both, becomes so deperate that their health, welfare and/or survival is at stake. Many foreigners, particularly those from such impoverished regions as Central America, understand all too well that coming to America is a difficult and dangerous process. Yet they are willing to assume those risks because they feel compelled to escape their horrendous conditions. Personally, I wish "immigration reformers" would factor these realities into their analyses before they decide whether imposing a new and comprehensive system of surveillance on all Americans is the appropriate approach for U.S. immigration policy.

The Private Sector

Given the profileration of the use of the SSN by federal and state governments, it's not surprising that the private sector organizations too increasingly have adopted it as their identifier. As mentioned, financial institutions now are required to record their customers' SSNs. But there are plenty of institutions that are not required but do so anyway.

As I was signing up for new natural gas service for my home the Gas Company phone representative asked me several questions and then asked for my SSN. I asked her why the company needed it. She said she wasn't sure. I suggested that we move onto to the next question. She agreed, and was able to provide me with gas service without me giving up my SSN. In the same week, I had nearly identical conversations with the phone represenatives of both the cable television and electric company. These companies do not really need the SSN, but everyone is so accustomed to asking for it, they do. And many people are so accustomed to giving it out, they do so without thinking about it.

Is there any harm? That depends on circumstance and the individual's point of view. I receive some two dozen calls a year from people who were irate about always being asked for their SSN.

Not only does the SSN make it easier for large institutions to compare their databases, it allows curious individuals (including private detectives, computer hackers or other strangers you might not want snooping into your private life) to "hop" from database to database and draw out a profile of your buying habits and personal lifestyle. The stranger might go to your

Department of Motor Vehicles and get your SSN from your publicly available driver's license. Then using the SSN, he might, albeit illegally, go to a credit bureau and find out what debts you owe, go to an insurance company or the Medical Information Bureau and find out about your health coverage and/or medical condition, check with various publishers to see what magazines you subscribe to and check with a few grocery stores trying out new computerized, "frequent buyer" progam to learn what you're buying habits. Access to credit bureaus is illegal, the laws are unenforced. There are few laws barring access to other private sector databases.

Some people do not really care who sees information about them. But as more people become aware of how much of their personal data are out there, they object to the ease with which it is gathered, swapped and stored.

Because current laws are weak, individuals have to be particularly vigilant to block the unnecessary collection of their Social Security number. Take the case of Don Pensa, a New Jersey resident, who recently told me his story. When Mr. Pensa learned that the New Jersey DMV was switching over to the SSN as the driver's license number, he appealed several times, even writing a letter, until he persuaded the department to grant him an alternative number. It was a difficult process, as the "whole place stood still" upon his suggestion of using a number other than a SSN, Pensa said.

Then, he convinced the Federal Aviation Administration that they did not need his SSN, but could grant him an alternative number for his pilot's license. Pensa reminded FAA officials that they assigned numbers to many foreign pilots who did not even have SSNs.

Next came the fuel oil company. When a phone representative insisted that the company would not open an oil delivery account unless he provided his SSN, Pensa said he would take his business elsewhere. The representative put him on hold for a minute, and then agreed that an account could be opened without an SSN.

Pensa said he was not as lucky with health insurance. In fact, he is still without health insurance because he cannot find an insurer who will provide him coverage if he does not provide his SSN, he said.

Some companies believe that using an SSN is convenient for themselves and their customers, and do not give much consideration to privacy issues. The Wall Street Journal reported February 4 that Fidelity Mutual Funds opened a computerized phone line permitting anyone to learn of a customer's fund holdings and balances by punching in the customer's SSN. A Fidelity marketing manager said the service was very popular and had only been the subject of three complaints. But after the story ran, Fidelity installed additional numbers for accessing the system.

Sunshine Is The Best Disinfectant

The media have exposed several questionable practices, causing private companies to alter them. One of the most significant was the public's response to reports about Lotus Marketplace: Households, the set of compact disks with personal data on 120 million Americans. The Washington Post reported that some 30,000 consumers told Lotus do remove their names and data before making the product available. This prompted Lotus, and its partner Equifax, the giant credit bureau, to decide the privacy outcry was too much and cancelled its plans to offer the product. When consumers asked how they could opt out, they were instructed that they needed to provide their SSNs, as the database feeding the system was operated by the credit bureau and keyed to SSNs. Similarly, Knight-Ridder exposed a Postal Service plan to keep persons' Christmas card mailing lists in a USPS computer.

In 1989, the New York Times exposed a secret program under which the Social Security Administration matched its database against sample databases submitted separately by Citibank and TRW, the credit bureau. After the story, and the issuance of Congressional Research Service Opinion that the program violated the federal Privacy Act, SSA ended the practice. Documents obtained by PRIVACY TIMES showed that both the match with Citibank and with TRW uncovered more than a 30 percent error rate among somebody's list of SSNs, presumably TRW's and Citibank's. This little-noticed fact raises questions about the accuracy of some private sector databases.

It also raises another issue: there is no real security for institutions in relying on the SSN. SSNs are too often transposed to create accidental inaccuracies. Moreover, individuals are pretty much free to get new SSNs.

The Privacy Act

The Privacy Act requires government agencies demanding SSNs to:
(1) cite its formal legal authority for using the number,
(2) reveal whether disclosure is mandatory or voluntary and
(3) explain how the number will be used.

I hope the above account makes it clear that the Privacy Act's "restrictions" on use of the SSN are of questionable value and that much stronger measures are needed if we are to restore to individuals and the SSN and privacy and integrity they deserve.

Some General Solutions

(1) There should be a moratorium on use of the SSN by all institutions not already authorized by law to use it.

(2) Create an independent national office to be in charge of U.S. privacy policy, to make legislative recommendations to Congress, to serve as a resource to the public and the media when they need information about or help with a privacy issue.

(3) Strenghten existing laws, like the Fair Credit Reporting Act, Right To Financial Privacy Act and Privacy Act, which are badly out of date and full of loopholes.

(4) Enact new laws in the most urgent areas in which people have few rights in relation to their personal data, particularly medical, insurance and employment records.

(5) Commence a public education campaign encouraging individuals to be vigilant about controlling their personal data. This campaign would be based upon the premise that institutions should not use personal data they collect from individuals without first obtaining that individual's informed consent.

I can't emphasize enough the importance of the United States having an independent office in charge of our national privacy policy. In other countries such offices have played important roles.

Two notable examples concerned limits on the use of identification numbers. A few years ago in Ottawa, then Privacy Commissioner John Grace recommeneded that the Canadian Government conduct a complete review of its agencies's use of their Social Insurance Number (SIN), and restrict its use when found to be unnecessary and inappropriate. Grace had no authority to order this change. But the Canadian Government carried out Grace's recommendation. For the first time it identified the ways in which the SIN was being used and actually halted its use in a few cases.

Last year, the Ontario Provincial Government adopted a new health identification number to be used by provincial citizens under the health plan. The Ontario Office of the Information and Privacy Commissioner studied the issue and recommended strict curbs on use of the number. The Government instituted the commissioner's recommendation as provincial policy.

SOME IDEAS FOR THE SUBCOMMITTEE

I hope you will hold additional hearings on the Social Security number and privacy issues. You will find that the attention you focus on the issue provides important public education and raises public awareness -- an important development in itself.

While we have some anecdotal evidence, we really do not have a comprehensive survey of how the SSN is used in the public and private sectors.

It would be important to know if federal agencies are complying with Section 7 of the Privacy Act, which concerns their obligation to inform individuals if disclosure of their SSNs is mandatory or voluntary. The section was intended by Congress to prohibit coercing individuals into divulging their SSN when it was not necessary. But it's not clear what impact this Section is having on agency practices. Perhaps the General Accounting Office could examine this issue. The GAO or Congressional Research Service also could list federal laws authorizing or requiring use of the SSN.

Similarly, we do not know the extent to which the SSN is used in the private sector for non-employment purposes. We also do not know to what extent advances in technology permit companies that use the SSN as a customer identification number to manipulate personal information and create consumer profiles.

One idea would be for the Office of Technology Assessment to do a study which would include a survey of the private sector and how the SSN and information technology impacts on consumers' privacy rights. Learning the extent of SSN usage in this context would help focus the issue and possibly assist in the development of corrective measures.

Mr. Chairman, again thank you for this opportunity to submit my views. Advancing the cause of privacy is an interest the entire public shares. An important part of advancing privacy is leadership by individual members of Congress. Sen. Sam Ervin's legendary efforts on behalf of privacy and justice are well known. Another Senator from Indiana, Sen. Birch Bayh, was a particular inspiration to me when I first came to Washington in 1977. He was active on several privacy issues. He began the legislative process which a few years ago resulted in a law banning the use of polygraph tests in most private sector workplaces.

I look forward to working with you in the future. I would be pleased to answer any questions.

Chairman Jacobs. Thank you, very much.

Ms. Baskin, you are not related to the ice cream people, are you?

Ms. Baskin. No, I am not an ice cream heiress, I am sorry to say, but I did keep them in business.

Chairman Jacobs. Do you know where the ice cream hails from? My coworker, Ms. Noe, tells me that you have information about a DeTec machine, a machine that you tell a Social Security number and they tell you your shoe size?

Ms. Baskin. Right. I was curious about the wrong Social Security number in one credit reporting agency and since I have not straightened it out, I wondered who it belonged to. So I called up a car dealer and they have a new gizmo that they have had for a little while, called DeTec and it tells you name changes, addresses, age, and the employers. And I ran the number that is wrong and it came out as no record found, that it was out of range. It is not a Social Security number that is in use.

But I am not sure that I should be able to do that. It is very handy for a reporter. I have run Social Security numbers before to find people and it is inappropriate, I know, but helpful to me in my career.

Chairman Jacobs. Don't do as I say.

What does the panel think about the new law with regard to newborn children, Social Security numbers, I mean? Do you see a problem in that? You see the reason for it, of course, but——

Ms. Baskin. Social Security numbers for?

Chairman Jacobs. For newborn children.

Ms. Baskin. I am pregnant and I have done genetic testing and I know that there is a medical file that already exists on my unborn child. The Social Security number could come next before she is born.

Mr. Hendricks. Well, the Social Security number there was established as a taxpayer identification number. In this case, it does create the life-long use of the Social Security number. I think what makes it a little better, from my point of view, is that it is for tax purposes, which is a key part of the Social Security number and it is not for a lot of these extraneous purposes. So that is a very narrow use and you have to get one sooner or later anyway.

Chairman Jacobs. We have an 18-month old and when we filed our taxes last year, I think he was about 6 months old, and we felt pretty important putting his Social Security number down even though I don't think it is required until age 2.

Which is the greater danger, exposure of your private affairs, your private matters and data or misidentification? I suppose the question almost answers itself. Mr. Wiggins would tell you that the second one is the greater danger. But how great is the danger about privacy? Since I can remember the question keeps crossing my mind in the case of classification of Government documents, what is the big secret? Well, of course, in that case the Government works for us and it shouldn't be very much secret from the Government to us, but from us to the Government.

What if I don't want anybody to know my shoe size for example?

Mr. Hendricks. Right, well, we don't have time to give the litany of horror stories and maybe we could submit more of that for the record so that you will have that too. I think the greater danger is the erosion of trust. People want to give information to one institution, and they think it is going to go there and only be used for that purpose. The great danger now is that it is being used for secondary purposes by all sorts of institutions without informing people that they are doing it and without obtaining their consent. There are too many large institutions visiting each other's back doors and taking out personal information on people.

And that there is a backlash building against that right now and there is going to be an erosion of trust in our society. Privacy is seldom for privacy's sake. A lot of times it is to actually increase participation and communication. You have a doctor and a patient who have a privilege, just like a lawyer and a client or a reporter and his source. And the reason that they have a confidentiality privilege is that so you can increase communication.

In the same way, I think our information practices need to adjust so that we can feel free to participate as Professor Culnan was saying in the economy without feeling that information about us is going to be used out of context.

Ms. CULNAN. I would like to add that the privacy issue is not unique to the Social Security number, because anything that can uniquely identify a person can cause the same issues to arise.

I agree with the trust issue. Jeff Rothfeder said at a conference last summer, a lot of people who have these data banks to be our "electronic friends," and, in fact, thus makes it very difficult for people to maintain any kind of distance around themselves, because the information is collected and it does move without people's knowledge. More education would help because people really don't know what is going on. Then when they find out, they feel, as a friend of mine says, as if they have been filmed in the shower without anybody telling them.

Then there is this huge backlash which causes great difficulties for the organization which happens to be at the end of the backlash. We saw that with the Lotus MarketPlace where they were very much stunned, Lotus and Equifax, because Equifax had been selling lists for some time, as do lots and lots of other companies.

And, in fact, consumers were just not aware. When they found out about this one instance, they literally went nuts. It caused a big problem and the product had to be withdrawn after a substantial investment by Equifax and Lotus.

Chairman JACOBS. Our colleague, Lee Hamilton, was taken to task a few years ago by the Courier Journal, a liberal paper across the water from his district, because unlike other members of our delegation in Indiana, he would not release or did not release his Federal income tax form. That was mentioned earlier in the testimony here. I thought his response was rather effective and so did the Courier Journal because it ran another editorial saying, we were hasty. And he simply made the point that when one releases one's income tax returns, that person has possibly told the world about family illnesses, for example.

That led my recollection of a very elderly Federal judge in Indiana, a story my father told during World War II. The judge was about to sentence a man convicted of a violation of some banking laws and he asked the man about his family. The man said he had one son. The judge asked "is he in the Service, and how old is he?" He is 25. Is he in the military service? No, he is not.

And why isn't he? And the defendant, who was about to be sentenced said, that is none of your GD business. And this was a Federal judge. He was taken aback and as a matter of fact, he took the lawyers back into the chambers and said, you had better explain to your client how much trouble he is in here. His lawyer said, well, you will never get him to say why that is. And the judge said, well, why is it? The lawyer said, well, his son has Down's syndrome.

So I mean there are as, Doctor McDermott pointed out, there are layers upon layers of ramifications ultimately. We start out big and brave thinking, gee, I have nothing to hide, you can look in my closet any place you want to look.

Yet, I am connected with people who don't have anything to hide in the criminal sense, but perhaps do in the social sense.

Ms. Baskin, I won't trouble the panel any further, but in the case of the dating bureau that turned the data over to commercial entities, was any redress sought and obtained because of the violation of the contract, the condition of the contract?

Ms. BASKIN. No. None of the consumers that we contacted—I mean they were outraged about it. They were angry about it and surprised that this information had been used. In many cases, they had only made inquiries. They had not even signed up for the service, they had just asked about it. And none of them got together in any way.

I think that what I have gotten back from consumers, we had over 300 phone calls from people who were very upset about the proliferation of information on them, and how it is abused. But they feel stymied. They were turning to me and asking what can we do about this? I tried to provide solutions in reports that I do and I didn't in this case. I sort of failed the public in a way.

Chairman JACOBS. Well, Mr. Wiggins has a lawsuit, I take it against the organization which harmed him. I just wondered if a legal action might lie all the more clearly in the case of those who did subscribe to the dating service, and thereby, formed a contract with certain terms and conditions, one of which was grievously violated?

Ms. BASKIN. I think that as litigious as our society is that most of the people that called me and expressed their frustration were just upset. They are not ready to go to court about it, but they want something done. Many of them said, there ought to be a law, that kind of thing, to protect them. People, I think, are most frustrated about the proliferation of mail that they are getting. I mean you have to fight your way in the door these days. There is some statistic that takes 9 months of your life to get through your junk mail and I am sure I spend more time than that. I seem to get four of everything with different names.

I have tried to opt out which is the only option that you have right now through the Direct Marketing Association and that has not been successful. I have heard from a lot of frustrated people about that.

Chairman JACOBS. We have a good friend who is a State Senator out in Indiana and when she was first elected to the House of Representatives there, she had signed a contract to have a heating system put in her home. They were using 4 inch pipes to deliver heat to the third floor of her home and for those of you who are not initiated into that business, they don't work.

And my father sued on the bond and got all her money back, got a good contractor, and she has got a nice heating system now. Just before she entered the legislature she asked my father well, is there not some law that we could pass to protect people like me from that? My father said, well, there is already a law Julia. And that is called a guardianship. And when you mentioned the ice cream and how people gave up their Social Security numbers for a little lick of ice cream, I think Sam Gibbons said, well, maybe those people need guardians.

So you can only go so far in protecting us from ourselves.

Well, I thank the panel very much. You have made very useful contributions.

I think that we only have one more panel today. This one consists of Janlori Goldman, Cecilia Munoz, David Simcox, and Dan Stein.

We will begin with Ms. Goldman.

STATEMENT OF JANLORI GOLDMAN, DIRECTOR, PRIVACY AND TECHNOLOGY PROJECT, AMERICAN CIVIL LIBERTIES UNION

Ms. Goldman. Thank you very much, Mr. Chairman.

My name is Janlori Goldman. I am the director of the American Civil Liberties Union Project on Privacy and Technology. I very much appreciate that you have invited us to testify today. We had the good fortune to work with your committee last year on the ID card provision of the Immigration Act that Senator Simpson testified about earlier this morning. I think that Senator Simpson, as well as a number of other Members of Congress, were very surprised at the deep and visceral opposition to the identification card proposal that the Senator inserted into the Immigration Act last Congress.

The proposal would have killed the bill, absolutely would have, had it not been removed. The ID card provision tapped the opposition that many people in this country have to a national ID card or any form of mandatory identification document.

Yet we see how identification technologies and ID cards are a part of our every day life. As a number of people have already testified, we give up our identification all the time.

The real issue here is not so much that the Social Security number is used as the identifier in data bases but that it was only created for one purpose. It was created for the very limited purpose of keeping track of Social Security data. Now, we see, as the Office of Technology Assessment found in a report recently, that it is a de facto national identifier. The problem is not that the number is used by individual companies, by TRW or by doctors or credit card companies, but that that is the key that unlocks information in other data bases. It allows for a disclosure of information from one file to another file. It allows information to be manipulated. It allows you to get information in another file because it is a unique identifier and because all these other services, all these other companies, all these other agencies are using the number as the identifier.

That is one of the reasons that TRW wanted the Social Security Administration to verify the Social Security numbers that they had. And under Dorcas Hardy's administration, a number of years ago, when it was disclosed that SSA was doing this, and for a profit, Senator Pryor held an oversight hearing, and raked them over the coals. He said, "this is against the law." This goes against the Privacy Act of 1974, and it violates peoples' privacy. SSA eventually stopped the verification practice.

TRW, by the way, does have a service called social search which allows you to use the Social Security number to find out people's current addresses. So they are not just providing this for credit reporting purposes and using it as the identifier to keep their files in order. They have other services that they are marketing with this information. Thus, it is important for them to have accurate Social Security numbers.

You asked a question of the other panel that is the most important one here. What is the privacy interest here? In the 1990s, the biggest privacy issue is that people want to maintain some control over the personal information about themselves that they give over when they do business with other people; when they apply for Government benefits, when they get a credit card, when they get a driver's license, they only want that information used for that one purpose. But that is absolutely not the case. There are few laws and few policies in place that prevent the information from being disclosed for other purposes. It is not that people have anything to hide, although that is the common misperception. It is that they want to be able to say who should know about me; how should they know about me; and did I give them the information?

In this day and age, the Social Security number really is the key that unlocks those data bases.

The two big ID card proposals that we have seen in the last few years—even though the general public does not know yet that Congress has seriously considered national identification card proposals, whether Senator Simpson wants to call them that or not, they certainly are—are in the gun control area and in the immigration context. We believe the ID card proposals would cause serious invasions of privacy; would probably cause discrimination in employment and a number of other areas; would be incredibly expensive, at least a couple of billion dollars, as the Social Security Commissioner testified today; and would be a real administrative nightmare.

The real problem though, of course, is that ID cards will not solve the problems. In the gun control area, for instance, the problem is that felons are able to get guns. So, some believe, if we create an ID card that allows for direct access to criminal history records we will solve the problem. The issue though is that 80 percent of all felons who buy guns buy them on the black market. They don't walk into K-Mart and buy their guns there. So how is this ID card going to solve that problem?

In immigration, the problem is that there are some people who are here illegally who are using false documents. So if we create a national ID card for everybody in this country we will solve the problem? No, because then what you have is problems with underlying documents. To get a national ID card you are going to have to submit a birth certificate and a driver's license in order to get the card. So there is the problem with fraudulent cards and inaccurate numbers. ID cards don't solve the problem. What they do is create more.

The last point that I would like to make is that everyone has talked about how an ID card would only be used for one purpose, it would be a limited purpose card, and we would not allow it for use by law enforcement. We know that is crazy. Existing data bases at the Federal Government level and in the private sector have often been created for a limited purpose and then used for other purposes. The temptation to use them is irresistible. So we would caution you.

One last point. We urge this committee to continue its oversight in this area, to examine disclosures of personal information and to limit the use of the Social Security number.

Thank you very much.

[The prepared statement follows:]

TESTIMONY OF JANLORI GOLDMAN
AMERICAN CIVIL LIBERTIES UNION

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to testify before you today on behalf of the American Civil Liberties Union (ACLU) Project on Privacy and Technology on the evolution of the Social Security number (SSN) into a national identifier and recent proposals to establish a national identification card. The ACLU is a nationwide, non-partisan organization of more than 275,000 members devoted to protecting the Bill of Rights.

The ACLU Project on Privacy and Technology, created in 1984, examines the impact of emerging technologies on individual privacy rights and other civil liberties.

I. INTRODUCTION AND OVERVIEW

Over the past fifty years, the SSN has evolved from a single-use identifier to the identification number of choice for the public and private sector. In this computer-driven era where information is connected to a single identifier, such as SSN, and entered into massive databases, it is possible to instantly exchange, compare, verify and link information in separate databases, often without the knowledge and consent of the person divulging the information. Such a storehouse of information, inevitably made accessible to federal agencies, state governments and private sector interests, presents a very real potential for abuse. Attempts to reverse the trend towards turning the SSN into a de facto national identification number have been largely unsuccessful. And, in recent years there have been proposals to establish a national identification card system in response to concerns over illegal immigration and gun control.

Proposals for a national identification card have often appeared a tempting "quick fix" to pressing national problems of keeping track of people, but the fact that no such card exists today is probably best explained by the visceral distrust with which most Americans react to the idea. For many, the prospect of being required to carry a national ID card conjures up the specter of "Big Brother"; of the government and the private sector collecting and maintaining an enormous amount of personal information and tracking our transactions and movements. People fear that this information can and will be used against them. The step from a mandatory identification system to a severe restriction on privacy and freedom may be a small one.

Most people are overwhelmed by the number of circumstances in which the SSN is requested, and people are not often informed about how the number can be used as the key to link information in other databases. Many people, particularly the generation that lived through the Second World War, are especially wary of using an identifier that allows the government and private sector to track their actions and identity.

For many Americans, knowing that the government has access to a broad range of information about them and can track their movements is very troubling. Political activists, in particular, who generally come into more direct contact with the government than the average citizen, have more to fear from such dossiers. Alan Westin wrote in his seminal book, Databanks in a Free Society that "many dissenting and minority groups in [American] society...view the establishment of such an identifier...as a giant step toward tightening government control over the citizen for repressive purposes."[1] A national ID card would increase the potential for abuse and misuse of personal information held by the government and the private sector. Barriers to the instant exchange, verification, and manipulation of the information would disappear. Large-scale information systems, even if created for a limited purpose, inevitably take on a life of their own -- the temptation to use the information for other purposes is irresistible.

The ACLU has vigorously opposed the creation of a national ID card. An ID card, we believe, would pose substantial threats to individual privacy and could be used in a discriminatory manner by employers and law enforcement. In addition, a national ID card would be an inherently unreliable form of personal identification, particularly if it used the SSN as the identifier. The poor quality of Social Security number records is well documented. In fact, any identification system is inherently unreliable since it based on the authenticity of the underlying information that individuals give to get the ID in the first place. Also, the government estimates the cost of putting an ID card system in place could cost billions of dollars.

Finally, we believe that a national ID card, in any form, will not be the quick-fix its proponents claim it to be for a host of social problems. A card is not a real solution -- it will only compound existing problems and create new ones.

---

[1] A. Westin, Databanks in a Free Society (1972).

II. THE SOCIAL SECURITY NUMBER

The SSN was created in 1935 solely for the purpose of tracking contributions to the social security fund, yet today it is required for most purposes when dealing with federal agencies, local and state governments, as well as for a wide range of private sector transactions. This unintended result occurred for a variety of reasons but it is important to note here that although Congress has consistently opposed the creation of a national ID card and sought to slow the growing use of the SSN, over time Congress has required the use of the number in seemingly small, unrelated contexts. The overall result has been, as the Congressional Office of Technology Assessment (OTA) concluded in 1986 that the SSN had become a "de facto national identifier." A history of the number's use shows the slow but inexorable move from a single to a multi-purpose identifier.

The Social Security Act required that the Social Security Administration keep records on millions of workers for the rest of their lives. Workers covered by the Social Security program were issued an account number, which they were then required to report to employers. In turn, employers then reported to the IRS information on wages paid and taxes withheld from their employees.

In a move towards efficient recordkeeping, President Roosevelt issued Executive Order 9397 in 1943, which encouraged federal agencies to use the SSN when establishing a "new system of permanent account numbers pertaining to individual persons." In 1961, the Civil Service Commission began using the number to identify all federal employees. The following year the IRS required the number on all individual tax returns. Widespread use of the number began in the mid-1960's, however, when the development of the computer coincided with burgeoning public assistance programs.

Over the next decade, the number's uses by the government and the private sector expanded dramatically. The SSN is required to apply for most government benefits and programs. The number is also required a wide variety of commercial transactions, including applying for credit, employment, insurance, as identification on a check and even to enroll in college.[2]

---

[2] In 1989, the New York legislature passed a law prohibiting merchants from asking customers for the social security number and other personal information when using a credit card. The law is intended to restrict the collection and sale of personal information for marketing purposes.

As the demand for the number grew, so did concern over its abuse. In 1971, a Social Security Administration Task Force issued a report decrying the run-away use of the social security number for identification purposes:

> The increasing universality of the social security number in computer data collection and exchange represents both substantial benefits and potential dangers to society; [a] national policy on computer data exchange and personal identification in America [is necessary], including a consideration of what safeguards are needed to protect individuals' rights of privacy and due process.

In addition, the Task Force questioned the desirability of "any kind of universal identification system in terms of its psychological impact on the individual citizen."

In the same year, the Senate Judiciary Subcommittee on Constitutional Rights held hearings on "Federal Data Banks, Computers and the Bill of Rights." Department of Health Education and Welfare (HEW) Secretary Elliot Richardson testified that while "[t]here would be an enormous convenience in having a single identifier for each individual...it is this very ease of assembling complete records, of course, which raises the specter of invasion of privacy."

During the Senate hearings, Committee members expressed surprise and outrage at the "secret" government databases they unearthed. For instance, HEW had compiled a blacklist of advisors and scientists that the Department refused to appoint to advisory boards. Even more distressing to the Committee was the discovery that the Army was using computers to conduct surveillance on people believed to be "political subversives." As Professor Arthur Miller testified: "It is not essential that dossiers, files, surveillance actually are used to repress people. If these activities give the appearance of repression, that in and of itself has a chilling effect on the precious rights guaranteed to us by the Constitution."

Two years later, in 1973, HEW issued a report entitled Records, Computers and the Rights of Citizens, warning that the creation of a standard universal identifier would lead to a national dossier system that could track people for a lifetime. The HEW report strongly opposed the implementation of a national identifier because an "uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems" had the potential to lead to invasions of privacy.

During the early 1970's, there was growing concern in both the executive and legislative branch, as well as among individual legal and privacy experts, that the expanding use of the SSN had unanticipated and threatening consequences for the privacy rights of all Americans. Congress responded by enacting the Privacy Act of 1974.

The Privacy Act was based on a congressional finding that the right to privacy, a personal and fundamental right protected by the United States Constitution, was "directly affected by the collection, maintenance, use and dissemination of personal information by federal agencies," and that the increasing use of computers and sophisticated information technology had "greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information."

To prevent the SSN from becoming a national identifier, the Privacy Act prohibits new uses of the number unless Congress itself authorized them. Congress feared that if the "use of the SSN as an identifier continues to expand, the incentives to link records and broaden access are likely to increase." The Senate Committee report described the growing use of the number as "one of the most serious manifestations of privacy concerns in the nation," including the risk that "the number may become a means of violating civil liberties by easing the way for intelligence and surveillance uses of the number for indexing or locating the person." Senator Barry Goldwater (R-AZ) spoke on the Senate floor in vehement opposition to the increasing use of the SSN, calling on his colleagues "to stop this drift toward reducing each person to a number."

To address privacy issues in more depth, the Privacy Act mandated the creation of the Privacy Protection Study Commission and empowered it to hold additional hearings. The Commission was required to study how the SSN is used to "identify individuals in databanks and to gain access to, integrate, or centralize information systems and files." In its 1977 report, Personal Privacy in an Information Society, the Commission found widespread opposition to the use of the SSN as a national identifier because individuals:

- resent being identified by a number rather than a name;
- fear that if several organizations possess an individual's SSN the ability with which those organizations can exchange information about the individual will be greatly facilitated, and
- are concerned that if the SSN is used to facilitate unconstrained exchanges of information about people, dossiers about individuals may be created that will follow them throughout life.

Seeing "a clear danger that a government record system, such as that maintained by the Social Security Administration or the Internal Revenue Service, will become a de facto central population register," the Commission's final recommendation was that the federal government "act positively to halt the incremental drift toward creation of a standard universal label and central population register until laws and policies regarding the use of records about individuals are developed and shown to be effective.

Despite the fact that Congress has specifically rejected the use of the SSN as a national identifier, it has played a large role in the number's expansion, authorizing and requiring it for many government programs. Recently, for example, Congress acted to increase the use of the number in the Tax Reform Act of 1988 which requires that children claimed as dependents on tax returns must have an SSN. The purpose behind this requirement is to catch parents who both claim children as dependents. Also, Congress authorized states to require the number as the identifier on drivers' licenses. In this way, the number has become the most widely used identification number.

However, significant differences exist between a de facto national identifier and a federally-issued national identification card. First, the SSN was never intended to be relied on by itself as foolproof identification. Historically, SSNs have been easy to obtain because there was no need for a secure card for Social Security Administration purposes. Second, despite growing use of the number, Congress has attempted to limit its use for fear that it was becoming a universal identifier. Third, as a practical matter, using the SSN for positive identification would pose administrative problems and potentially cost billions of dollars. Due to the large number of inaccurate and duplicate numbers, the number would have to reissued if it were to be effective at all. And, most importantly, an ID card could subject people to privacy intrusions, such as government surveillance and increased data collection and sharing.

There are clear examples of how government-collected information has been used for a purpose other than that for which it was initially intended. For instance, the confidentiality of Census Bureau information was violated during World War II to help the War Department locate Japanese-Americans so they could be forcibly moved to internment camps. And, during the Watergate years there were illegal disclosures and uses of Internal Revenue Service documents and other government records for political purposes. During the Vietnam War, the FBI secretly operated the "Stop Index" by using its computerized National Crime Information Center (NCIC) to track and monitor the activities of people opposed to the United State's involvement in the war.

The government has also shared its information on individuals with the private sector. The FBI's criminal history records system, which started out being limited to law enforcement uses, is now being used more and more by employers and licensing boards. In fact, approximately half of the requests the FBI receives for criminal history records today are from non-law enforcement agencies, including many private sector employers.

Also, the Social Security Administration (SSA) used to disclose SSNs to the private sector until public disclosure halted the activity. Two years ago, it was discovered that the SSA had been in the business of using the SSA's massive data files to verify SSNs for commercial purposes. Following public disclosures, the SSA Commissioner announced in April, 1989 that the agency decided not to process magnetic tapes containing 140 million names and SSNs submitted by TRW Credit Data, a credit reporting company.[3] At a Senate hearing on the matter, Senator David Pryor expressed outrage at the earlier verifications, saying the agency had violated peoples' right of privacy. Pryor chastised the Commissioner: "As far as I'm concerned, this is as far away from the mission of the S.S.A. as anything I've ever heard of."[4] Senator Pryor commended SSA on its decision to halt verification of social security numbers for businesses:

> "I am glad that Commissioner Hardy has taken this path and seen fit to preserve the confidentiality of the Social Security files. Unfortunately,...this action comes too late to protect some 150,000 people whose files were violated during a test run for TRW and for more than three million people on whom verifications were conducted for Citibank and other firms in past years."[5]

The private sector's use of the social security number to access information about individuals has evolved to a point never envisioned by its creators. For example, in a 1990 advertising brochure, TRW Credit Data, which holds itself out as the nation's largest provider of consumer credit information and claims to maintain information on nearly 170 million consumers nationwide, advertises a service called Social Search:

> In pursuit of those who have disappeared - former customers, college alumni or missing shareholders - TRW brings you Social Search: A state-of-the-art locating tool that puts our expansive databases to work for you . . . All you need

---

[3] Washington Post, April 14, 1989 at A-10.

[4] New York Times, April 15, 1990, at 1.

[5] Id.

> are the Social Security numbers of those you're attempting to locate and you can reach those hard-to-find individuals who may have moved or changed their names.

III. CURRENT ID CARD PROPOSALS

In recent years, there have been efforts in Congress to create some form of national identification card as the "quick-fix" to sweeping social problems, such as illegal immigration and gun control. In both contexts, the ID card proposals were defeated on the grounds they posed grave threats to privacy, could be used in a discriminatory in employment and by law enforcement, and were impractical, unreliable and costly. In essence, the creation of an ID card system could not be justified when balanced against the cost to civil liberties and government administration. Nevertheless, we believe similar versions of these ID card proposals will resurface this Congress.

A. Immigration Reform

Under the Immigration Reform and Control Act (IRCA) of 1986, employers are required to verify the identity of potential employees and their eligibility to work in the U.S. A host of documents are acceptable to use, including passports, birth certificates, driver's licenses, voter registration cards and Social Security cards. Employers may be liable for sanctions for failing to comply with the verification requirements.

When Congress passed IRCA, it explicitly declined to authorize the establishment of a national identification card as a means of enforcement:

> Nothing in this section shall be construed to authorize directly or indirectly, the issuance or use of a national identification card or the establishment of a national identification card.[6]

During debate on IRCA, Senator Alan Cranston (D-CA) predicted on the Senate floor at the time that the failure of employer sanctions would lead a future Congress to enact a national identification card:

> Employer sanctions can be the first step toward a national identification card-internal passport system - a primary tool of totalitarian governments to restrict the freedom of its citizens. And, when employer sanctions are discovered

---

[6] 8 U.S.C. 1324(c)(1989).

not to be working...that is when the danger of taking the second step occurs.[7]

As Senator Cranston predicted, debate over the national ID card has recently been revived in response to the problems arising from the employers sanction provisions of IRCA. A number of reports have concluded recently that employer sanctions have led to an increase in discrimination against racial and ethnic minorities. It appears that employers are concerned about the authenticity of documents used to verify the identity and status of prospective employees.

In the 101st Congress, a number of bills were introduced to create both voluntary and mandatory identification/work authorization cards to ease confusion over the reliability of existing documents. The bills' proponents claimed that a government-issued ID card will make it easier to enforce sanctions by ensuring the card cannot be faked.

The ID card proposal that came closest to becoming law was inserted by Senator Allan Simpson (R-WY) during the conference on the Immigration Act of 1990. The provision called for an ID card/driver's license pilot program, using the SSN and biometric identification, such as a fingerprint. The card was intended as a document that could establish work authorization and identity. During eleventh hour negotiations, the ID card provision was dropped after strenuous opposition from the civil rights and immigrant's rights communities.

In addition, there were proposals to create a federally-issued, voluntary work authorization card, that could be used to satisfy the requirements under IRCA. Proponents of the voluntary card intended it to be used by people who might fear employer discrimination against minorities. Despite this laudable goal, the vast majority of witnesses who testified at a hearing on one such measure, vigorously opposed it, citing concerns about increased discrimination, invasions of privacy, security and reliability of the card and the system needed to sustain it, cost, need, effectiveness, and the premature nature of the proposal.

A voluntary card poses substantial risks of becoming a de facto mandatory minority-only identification card. Although intended to enforce employer sanctions against hiring undocumented workers while avoiding employer discrimination on racial or ethnic grounds, a "voluntary" card for minorities would instead have the effect of requiring legal residents and American-born Hispanics and Asians to carry a card proving their bona fides, while Caucasian Americans would likely obtain employment without having to produce a card.

---

[7] 132 Cong. Rec. S16904 (daily ed. Oct. 17, 1986).

All of the proposals, but particularly the creation of a mandatory national identification card, would require the establishment of a central computer system to store the information gathered on individual card bearers.

Perhaps the greatest problem that these proposals fail to solve however is that any identification card will be inherently unreliable because it would depend on the use of underlying documents such as a social security card or driver's license, both of which are notoriously unreliable and vulnerable to fraud.

B. Gun Control

In addition, the national ID card solution has been proposed to regulate the sale of firearms. A recent law, known as the "McCollum Amendment," requires the creation of a system for the "immediate and accurate identification of felons who attempt to buy guns." The law requires the Attorney General to report to the Congress on the feasibility of creating such a system. A Justice Department Task Force issued a report outlining a range of options for implementing the law.

One option was to create a number of different identification cards to be carried by people eligible to buy guns, including a Firearm Owner's Identification card (FOID) to be issued to all potential gun buyers who passed a fingerprint clearance test. The FOID card met with substantial resistance in that it targeted potential gun buyers to carry a special ID card. Opponents worried that this group would become the subject of increased investigations. A "voluntary" card for firearm owners would establish another unsecured database with no guarantees that such information would be used for unintended purposes.

As an alternative to the FOID card, the Justice Department offered its most sweeping proposal -- a requirement that every person living in the country carry a "smart card" containing "biometric data and information such as felony convictions that would legally bar someone from purchasing a firearm." The Task Force did cite excessive cost and "substantial public resistance to the requirement to carry such a card, especially since the need for interstate coordination may require the creation of biometric databases for the nation's adult population."

Most importantly, even if implemented, all of the Task Force's proposals would be nearly useless. None of the identification proposals would actually prevent felons from buying guns since over 80% of felons purchase firearms through the black market and not through licensed gun dealers.

the registration card for [illegible] smart card for all citizens, denouncing the proposals as "an infringement on the rights of Americans."[8]

IV. PRIVACY IMPLICATIONS: THE THREAT OF LINKING INFORMATION

A mandatory national identification card poses substantial concerns for individual privacy and civil liberties, and would be unreliable and extremely costly. A "tamperproof" card, unique to each individual, would be feasible only with vastly increased data collection necessary to bolster the card's credibility. Before such a card could be issued, people would have to present personal information as to their identity, citizenship status, and possibly a biometric identifier such as a fingerprint.

The underlying documentation needed to verify a national identification card will require the creation of a national databank containing personal information on every individual in the United States. Such a system would provide the government and private institutions with the ability to track and profile people from birth to death, creating what Professor Arthur Miller termed a "womb-to-tomb dossier."

A national identification system will inevitably lead to the sharing and manipulation of personal information for purposes other than verifying identity. Using the card as the key to unlock personal records held on individuals, the government and the private sector will be able to engage in activities that go far beyond the purpose of the card. For instance, if the card is established for work authorization purposes, the temptation will be irresistible to make the database available to federal agencies other than the INS. In fact, a recent study that proposes the creation of a national work authorization card makes that recommendation: "[F]uture legislation should permit greater flexibility for use of work authorization data, under adequate safeguards, for broader public administration and law enforcement purposes."[9] Once the system is in place, it will undoubtedly take on a life of its own.

---

[8] Washington Post, June 29, 1989, at A-41.

[9] D. Simcox, Secure Identification: A National Need - A Must for Immigration Control, Center for Immigration Studies, 1989.

V. A NATIONAL ID CARD: A DOMESTIC PASSPORT

A national identification card may become a de facto domestic passport. As a supposedly tamperproof form of government-issued identification, it would inevitably become the card of choice for law enforcement officials who will request the card from individuals to prove their identity and legal status. Understandably, many Hispanics, Asians, resident aliens and others are likely to feel an implicit requirement that they always carry their card. In addition, people who fear police harassment or intimidation may feel especially vulnerable to a need to carry the card as a means of self-protection.

Recent developments in constitutional law increase the prospect that a national identity card would be transformed into a de facto domestic passport. Under many circumstances, law enforcement officials could approach individuals and ask them to produce such a card without any specific, objective basis for suspecting illegal activity. As a result, there would be little judicial scrutiny of the extent to which race or ethnic appearance might affect decisions to single out individuals for such requests. In addition, failure to produce the identity card might form the basis for both further investigatory detention and perhaps even an arrest and full personal search.

VI. OTHER COUNTRIES

Many countries have SSN equivalents that are used by the government for tax and public benefit purposes, such as Canada, the United Kingdom, and Australia, but the use of the number is limited. Further, most countries that do have an identification card system, such as Germany and France, limit uses of the card and maintain decentralized systems. Recent efforts in Australia and the United Kingdom to issue ID cards were met with strong opposition and were ultimately defeated.

A common thread between most countries is that various numbers are used for various purposes, and the governments' administration of these systems is often unconnected and decentralized. For instance, in the Federal Republic of Germany, an identification number and card of a "general multi-purpose nature [are] regarded as being an anathema to self dignity."[10] Germany has resisted proposals for a centralized identification number as leading to social control through interconnecting files. France has also resisted centralizing and automating its

---

[10] CJ-PD at 2. Committee of Experts on Data Protection for the Council of Europe, "The Introduction and Use of Personal Identification Numbers." (CJ-PD, March 23, 1990).

ID system based on the "real danger for the liberty of individuals."

VII. DATA QUALITY AND COST

As the information collected on individuals and the number of individuals increases, the problems that result from human error will increase exponentially. Mistakes in data entry, mistaken matches of information, and data either mistakenly or willfully divulged, will inevitably result in embarrassment, inconvenience, and more serious infringements on people's rights. Furthermore, even extremely sophisticated technology cannot overcome the central problem that makes current identification cards unreliable - the ease of obtaining fraudulent underlying documents such as birth certificates, driver's licenses, and SSNs.

The SSN is a notoriously unreliable identifier. Of the over 210 million SSns in use today, about 75 percent were issued before evidence of age, identity, and citizenship or alien status were required. Only 76 million of the initial and replacement social security cards have been issued using the new counterfeit and tamper-resistant paper, so that most cards in use are easy to alter or forge. And, there is no method to positively assure that any person presenting a social security card is the person to whom it was issued since the card contains only a name, SSN, and signature.

In addition to the problems inherent in creating a national identification system, there is the cost of implementing such a system. For instance, the General Accounting Office estimates that re-issuing 210 million new "counterfeit-resistant" social security cards would cost billions of dollars.

But most importantly, the recent proponents of national identification cards in both the context of gun control and immigration law have not carried the burden of persuasion on the fundamental issue of whether the card would remedy the problems it is intended to solve. In the final analysis, the establishment of a national identification card, with the necessary accompanying database, is a "solution" that threatens to create more serious problems than it solves.

VIII. CONCLUSION

The ACLU commends this Subcommittee for holding this very important and comprehensive hearing on the burgeoning use of the SSN and proposals to create a national ID card. We urge you to oppose future efforts to establish a national identification system and we pledge to work with you in this endeavor.

Chairman Jacobs. Ms. Munoz.

STATEMENT OF CECILIA MUNOZ, SENIOR IMMIGRATION POLICY ANALYST, NATIONAL COUNCIL OF LA RAZA

Ms. Munoz. Thank you, very much, Mr. Chairman.

My name is Cecilia Munoz and I am the senior immigration policy analyst for the National Council of La Raza. We are a Hispanic policy and advocacy organization that represents about 128 community-based groups. I am here to address the notion of a national ID card or some kind of identifier in the immigration context, because it is on an immigration bill and in the course of an immigration debate that this has been proposed most recently.

The National Council of La Raza, as well as many other Hispanic, Asian, religious, civil rights, and other institutions sat before the Immigration Subcommittees in both the House and the Senate, prior to the enactment of the Immigration Reform and Control Act of 1986, or IRCA, to talk about the employer sanctions policy—this is the policy around which the ID card is coming up to argue both that it would be ineffective and that it would cause massive levels of discrimination against Hispanics, Asians, Caribbean blacks, and other people who appear foreign in this society.

We sit before this committee today to say that unfortunately our predictions have come true. The employer sanctions policy has not proven effective in controlling illegal immigration and it has caused massive levels of discrimination against our community. The ID card, interestingly, has been raised as a response to both of these problems. It is being posited by people like Senator Simpson as a way to strengthen employer sanctions by preventing document fraud. It is also being posited by some as a way of controlling the discrimination problem; some of the discrimination seems to occur because employers are confused about the number of documents that one can present to establish work authorization.

We are sitting before this committee to again say that the ID card proposal would neither solve the document fraud problem, nor would it solve the discrimination problem. We believe that it is very, very likely to cause greater levels of discrimination against our community. It is for that reason that you saw absolutely massive opposition to the ID card proposal when it was raised in the immigration debate last year. That is a true reflection of how the Hispanic community, in particular, feels about such a proposal. And I want to use one specific example which explains why the emotion is so intense.

Your colleague, Representative De la Garza, in the House of Representatives, as well as my boss, NCLR President Raul Yzaguirre, have had to carry ID cards growing up in south Texas, because they are Hispanic. They had to use ID cards to prove their identity in order to prevent them from being confused with undocumented workers, for example, despite the fact that in my boss' case his family has been in Texas since 1710. This is a community which is used to carrying ID cards. It is used to them being misused; used for law enforcement purposes of other types. This community, which sees itself as American, gets pretty tired of having to prove on paper that we are Americans simply because our names seem different or because we appear to be different.

Documents and document checking are the cause of the discrimination which has resulted from IRCA. Though Senator Simpson points out correctly that the law requires employers to check everyone's documents, it is logical and understandable, that if you as an employer, were faced with somebody with my last name and somebody with the last name like Jones, you would be more likely to check my documents because my name seems foreign to you.

That's exactly what is happening. We don't see how a new kind of ID card that everybody would have to carry is going to stop that practice from occurring. It is a discriminatory practice, it is a result of misunderstanding and other kinds of problems and an ID card simply won't fix it.

We are also convinced that an ID card will create more discrimination against the Hispanic community, as my colleague, Ms. Goldman points out, in the process of obtaining or replacing the underlying documents which would be necessary to secure such a card. Again, my birth certificate from Detroit, Mich., with the name like Maria Cecilia Munoz Sierra is going to be a lot more suspect because it looks like a Xerox of something than the birth certificate of somebody whose name is John Smith.

Again that is a reality in our society which we simply must not exacerbate by enacting new Federal policies. Hispanics are very upset that Congress has already passed a Federal law over our objections which has caused civil rights violations against our community. We are again alarmed that it is being proposed that we should endure more civil rights violations in the name of immigration control.

It is particularly upsetting because we don't believe that such a proposal will actually advance the cause of immigration control.

Again, there is a problem with underlying documents; even if this country were to adopt a policy where every document somehow were to be secure—which I think would be difficult to do—what it will do is simply push the undocumented population further underground. That is exactly what has happened as a result of employer sanctions. I think the failure of the so-called Latin Investment Bank in Washington, D.C., where thousands of Salvadorans were banking in this city, because they did not require Social Security numbers shows how this law is making people more exploitable and pushing them further underground. Clearly this kind of scorched-earth documents policy would do the same thing. It won't stop the problem. It will create a lot more problems for our community.

Thank you, very much.

[The prepared statement follows:]

STATEMENT OF CECILIA MUNOZ, SENIOR IMMIGRATION POLICY ANALYST NATIONAL COUNCIL OF LA RAZA

I. INTRODUCTION

Good Morning, Mr. Chairman and members of the Subcommittee, I am Cecilia Muñoz, Senior Immigration Policy Analyst at the National Council of La Raza (NCLR). NCLR is a Washington D.C.-based national organization dedicated to improving life opportunities for Hispanics in the United States. The Council serves as a national umbrella organization for 128 local "affiliates" -- Hispanic community-based groups which provide employment, education, health, housing, immigration, and social services to over one million Hispanics annually. NCLR has a long history of interest in immigration issues; Hispanics represent both the first and the most recent immigrants to the United States. The Council was actively involved in the debate which led to the Immigration Reform and Control Act of 1986 (IRCA), and many NCLR affiliates assist immigrants in the legalization process. In addition, NCLR has been actively involved in monitoring the discrimination which has resulted from the employer sanctions provisions of IRCA, and the various proposals for national ID cards which have emerged alternately as methods of strengthening employer sanctions policy and of mitigating the resulting discrimination. We are pleased that the Subcommittee is giving due consideration to this critical matter, and we are delighted to have the opportunity to testify.

II. BACKGROUND

The question of developing some kind of national identifier or a national ID card has been raised as a part of the immigration debate since the early 1980s, when the Select Commission on Immigration and Refugee Policy developed the policy proposals which became the basis for the Immigration Reform and Control Act of 1986 (IRCA).[1] The ID card question continued to emerge around the employer sanctions provisions recommended by the Select Commission and enacted as part of IRCA. Employer sanctions, intended to control illegal immigration by making it more difficult for undocumented workers to find jobs in the U.S., require employers to check the documents of all of their new employees,in order to verify their eligibility to work in the United States. Many proponents of some form of national identification system -- an ID card, a "phone-in" system, a standardized drivers license, and a more secure and universal social security card have all been proposed -- argue that such a system would strengthen employer sanctions by making it more difficult for undocumented workers to use counterfeit documents to find jobs in the United States. Nevertheless, when Congress enacted IRCA it specifically stated that the legislation was in no way intended to endorse or lead to the development of a more comprehensive identification system, primarily because the bill's proponents recognized the controversial nature of ID card proposals.[2]

The employer sanctions policy has had a major, purportedly unintended, side effect which has also fueled proposals for some form of ID card. Over a dozen separate studies, culminating in a 1990 report by the U.S. General Accounting Office (GAO) have concluded that employer sanctions have caused a widespread pattern of discrimination against Hispanics, Asians, and other Americans who appear "foreign" to their employers.[3] The growing evidence of discrimination has led to proposals for some form of ID card which would, proponents claim, alleviate the problem of discrimination which has resulted from this policy. A proposal for a "voluntary" identification card received little enthusiasm when it was proposed in the Subcommittee on Immigration, Refugees and International Law in the 101st Congress. Opponents of the idea, including NCLR, argued that a "voluntary" card was likely to be mandatory only for those who are experiencing discrimination under employer sanctions, which would probably be ineffective, and would create new forms of discrimination.[4]

---

[1] U.S. Immigration Policy and the National Interest, Select Commission on Immigration and Refugee Policy, March 1, 1981.

[2] The Immigration Reform and Control Act of 1986, PL 99-603, (November 6, 1986).

[3] See Unfinished Business: The Immigration Reform and Control Act of 1986, National Council of La Raza, December 1990, for a summary of the major studies on discrimination caused by employer sanctions.

Most recently, a proposed "pilot program" which would have required three states to develop a comprehensive ID card based on the drivers license became the basis for an emotional eleventh-hour debate on the rule preceding enactment of the Immigration Act of 1990 which nearly killed the legislation. The Congressional Hispanic Caucus led the charge to defeat the rule because of strong sentiment that any form of ID card is likely to have a negative effect on the Hispanic community, and because neither body of Congress had been given the opportunity to vote on the matter or consider it in hearings.[5] This most recent battle over a modest ID card proposal provides an example of the Hispanic-American community's profound opposition to any form of identification system, particularly one which is raised in an immigration context.

III. ID CARD AS A PROPOSED REMEDY FOR DISCRIMINATION

A. Discriminatory Practices under Employer Sanctions

The multitude of studies which illustrate the discriminatory effects of employer sanctions show that some -- but not all -- of the problems created by the policy arise from its documentation requirements. Under the law, each employer is required to verify the employment eligibility of new-hires by completing INS Form I-9, which lists a number of the documents which establish authorization to work in the U.S. Technically, employers are required to check the documents of all new employees once the hiring process has occurred. Unfortunately, there is ample evidence that employers, simply to protect themselves, have adopted hiring practices which result in employment discrimination and lost job opportunities for "foreign-looking" American citizens and other legally authorized workers.

According to the various studies which document discrimination caused by employer sanctions, there are several major discriminatory behaviors which have been adopted by employers as a result of the law:

- **"Citizens only" policies** - According to a 1990 GAO report, 14.7% of employers surveyed responded to the enactment employer sanctions by adopting a policy to hire only persons born in the United States.[6] Such a policy excludes large numbers of persons who are legally authorized to work, but are not U.S. citizens;

- **Selective checking of documents** - According to the GAO survey. 8.6% of employers surveyed responded to employer sanctions by checking the documents only of employees with a "foreign" appearance or accent;

- **Applying extra scrutiny to the documents of "suspect" persons** - Several studies which focused on cities with large immigrant populations, like Los Angeles and New York found that the documents of "foreign looking" persons were more likely to be considered suspect, and that many legally authorized workers -- including Puerto Ricans, who are U.S. citizens by birth -- were being asked to produce more documents even after they had established their right to work in the U.S.;[7]

---

[4] "Testimony on the Adoption of a Voluntary Work Authorization Card as Proposed in H.R. 3374," National Council of La Raza, 11/9/89.

[5] *Congressional Record*, Daily Edition, October 26, 1990, pp. H12980-12987.

[6] GAO 1990.

[7] Coalition for Humane Immigrant Rights of Los Angeles, Update: The Effects of Employer Sanctions on Workers, July 1989; the City of New York Commission on Human Rights,

- **Avoiding "foreign sounding" job applicants** - Hiring audits were conducted in New York and Los Angeles by civil rights organizations, and in Chicago by the GAO; all found that when accented and non-accented callers with similar qualifications inquired about entry-level jobs, those with even slight accents were treated vastly differently than similarly-qualified callers without accents.[8] In addition, the GAO survey found that 6.6% of employers admitted to staying away from "foreign" looking or sounding job applicants.

The evidence of discrimination, and other studies of the implementation of employer sanctions suggest that there are a number of ways to explain why employers have responded to the law by adopting discriminatory hiring practices. Perhaps most significant, it is abundantly clear that employers do not fully understand the law or their obligations under it. Many employers are staying away from "foreign-looking" persons simply out of confusion, or out of fear of enforcement of employer sanctions. In addition, there is widespread evidence that the number of documents which establish work authorization is confusing, which leads many employers to reject documents which are perfectly valid. Finally and unfortunately, it is also true that employer sanctions have provided a means for employers who were inclined to discriminate against Hispanics to do so for seemingly "legitimate" reasons.

B. A national identifier would not materially reduce discrimination

Because of the extensive evidence that employer sanctions have caused discrimination, the GAO and others have proposed that the social security card, some other document, or the social security number be used in a system to provide one single method of identifying workers and their eligibility to work in the United States. The philosophy behind such a proposal is that employers, who are currently presented with a confusing array of documents to prove work authorization, will be less likely to behave in discriminatory ways if they are confident that everyone has the same document, and they are able to recognize it.

A uniform document might reduce discrimination only in those cases where employers are rejecting unfamiliar documents or asking for additional documentation from Hispanic and Asian applicants; however, such a document would almost certainly not affect other discriminatory behaviors which have erupted since the enactment of IRCA. For example, GAO reports from 1988 and 1990 indicate that employers, though required to check the documents of all new hires, are selectively checking the documents of employees whose appearance, name, or accent suggests that they are foreign.[9] Providing everyone with the same document does not appear likely to change this discriminatory behavior.

Similarly, the results of three separate hiring audits indicate that employers are screening out applicants with foreign accents even before the application process begins. Because these discriminatory practices occur long before documents must be checked, it is clear that the adoption of a new ID system will not reduce this type of discrimination. The communities whose civil rights have been violated as a result of the enactment of employer sanctions are unwilling to accept the adoption of new policies designed to "fix" the law, particularly given the likelihood that, at best, they will only alleviate part of the problem. Indeed, the ethnic communities affected, many religious and professional organizations, and much of the civil rights community believe strongly that the only proper response to the ineffective, discriminatory employer sanctions policy is to repeal it immediately.

Tarnishing the Golden Door: A report on the widespread discrimination against immigrants and persons perceived as immigrants which has resulted from the Immigration Reform and Control Act of 1986, August 1989.

[8] Coalition on Humane Immigrant Rights of Los Angeles; City of New York Commission on Human Rights; GAO 1990.

[9] U.S. General Accounting Office, Immigration Reform: Status of Implementing Employer Sanctions after Second Year, November 1988; GAO 1990.

C. National ID system will lead to new forms of discrimination

It is abundantly clear to those who have suffered discrimination as a result of employer sanctions as well as the kinds of discrimination which have unfortunately plagued this society throughout its history, that the adoption of a national ID system of any kind will lead to new forms of discrimination. Many Hispanic Americans, including Congressman Kika de la Garza (D-TX) and NCLR President Raul Yzaguirre, have experienced routine misuse of identification cards in border areas, where U.S. citizen Hispanics were once encouraged to carry cards to prevent being mistakenly classified as undocumented immigrants and subsequently detained or deported. Random document inspections and searches of Hispanics at border checkpoints are already common; with use of a national identifier, such procedures are likely to be adopted in areas away from the border. Failure to carry a card at all times could be perceived as a reason for search, detention, or arrest. Even a card which is designed for use only in the context of a job search, by its very existence, is likely to be used more expansively, at the expense of the Hispanic community.

In addition, the very process of obtaining such a card is likely to cause problems for Hispanics. To the extent that fraudulent work authorization documents now undermine the enforcement of employer sanctions, one would expect a secure work authorization document system to become dependent on the security of underlying documents. These underlying documents, which would inevitably be necessary to obtain an ID card are, therefore, the key to its security and successful implementation. However, adopting such a policy could mean that the use of fraudulent documents, or the discriminatory treatment of "foreign-looking" persons would re-emerge around the process of obtaining underlying documents.

For example, proponents of a national identity card have argued that birth certificates -- which are not uniform even throughout the U.S. much less in other countries -- could be forged with relative ease, and thus used to obtain the ID document. The mere discussion of such a notion increases the likelihood that the birth certificates of "foreign-looking" persons will be considered suspect. The birth certificates of Hispanic-Americans, therefore, could be subject to excessive scrutiny. Persons who appear "likely to be undocumented" by virtue of appearance or speech accent may be required to present more supporting documents than their Anglo counterparts, and could be subject to delays in receiving the card while their documents are checked.[10] Such a system could, therefore, merely transfer the discrimination which is already occurring in the hiring process, to the process of obtaining a card.

Furthermore, under employer sanctions, many Hispanic Americans are experiencing excessive delays in obtaining documents which damage their opportunities to find jobs. For example, since the enactment of IRCA, many Puerto Ricans have experienced difficulty obtaining jobs because of six to eight week delays in receiving copies of their birth certificates from Puerto Rico.[11] Under a comprehensive ID system, there are likely to be further delays in verifying or obtaining underlying documents, which will cause great hardship for those whose employers are requiring cards in order to obtain a job.

IV. ID CARD AS METHOD OF STRENGTHENING EMPLOYER SANCTIONS

A. Inherent weaknesses in the policy

A national identifier was first proposed in the immigration context as a means of ensuring the effectiveness of employer sanctions, by making it difficult for undocumented workers to skirt the new law by using forged documents to establish work authorization.[12] While such a proposal may address one of the weaknesses of employer sanctions, examinations of the policy suggest that it is inherently flawed; there are much more significant deficiencies in employer sanctions which make them unlikely to be effective, even if a "forge-proof" document were developed.

---

[10] The Institute for Public Representation, Memorandum to the National Council of La Raza, Georgetown University Law School, November 7, 1989.

[11] Letter from Howard Golden, President of the Borough of Brooklyn, to The Honorable Rafael Hernandez-Colon, Governor of Puerto Rico, March 28, 1989.

First, perhaps the most fatal flaw of the employer sanctions policy to reduce illegal immigration is that it attempts to deal only with the market which "attracts" immigrant labor, without taking into account the factors which encourage migration from the home country. For example, Wayne Cornelius, of the Center for U.S.-Mexican Studies has done extensive research on the nature of the population likely to migrate and their reactions to the enactment of IRCA. His work identifies specific "sending communities" for which migration has been a survival strategy for decades, and finds that the propensity to migrate has not changed since the enactment of employer sanctions.[13] The arrival of large numbers of Central Americans who have entered the U.S. through the Southern border in the years since the implementation of IRCA also shows that factors at home which encourage migration have proven to be much stronger than the laws within the U.S. which attempt to control it.

In addition, there is scant evidence to suggest that employer sanctions really are changing the conditions within the U.S. which encourage undocumented immigration. An interim report prepared for the Department of Labor. for example, has found that employer sanctions have had very little effect in changing the labor market conditions which encourage illegal migration, and are unlikely to significantly alter the labor market.[14] Similarly, data on the level of apprehensions at the Southern U.S. border clearly show that, though illegal crossings diminished somewhat in the year immediately following enactment of IRCA, they have begun to rise again in recent years, matching their peak 1986 levels in some border areas.[15] Clearly, border crossings and tension at the border are on the rise, suggesting that the long-term effects of employer sanctions on reducing illegal entries are negligible.

A second and severe problem with employer sanctions is the very implementation of the policy. A recent study released by NCLR, *Unfinished Business: The Immigration Reform and Control Act of 1986*, contains an extensive analysis of the implementation of employer sanctions by the Immigration and Naturalization Service. Using data compiled by the GAO, NCLR found that, even though the INS had more than doubled its employer education efforts in the period between 1988 and 1990, employer understanding of the law dropped by as much as 26 percentage points during that period.[16] The effectiveness of employer sanctions, like U.S. tax policy, is heavily dependent on employer understanding of the law, compliance with its requirements, and fear of enforcement of its penalties. Yet the INS has actually reduced its employer education efforts since 1990, after disappointing results prior to that period.

In addition, several studies by the Rand Corporation and Urban Institute indicate that sanctions enforcement has been uneven and could lead employers to believe that they do not have to fear enforcement of the law.[17] According to all available evidence, the documentation requirements of sanctions are not and are not likely to become an employment standard for which employers expect to be held accountable.[18] The very nature of the INS, which is primarily responsible for the implementation of sanctions, further suggests that the prospects for the success of the policy are dim. It is widely recognized that the INS has severe bureaucratic and management problems which have consistently affected its ability to enforce pre-IRCA immigration laws and provide services; it is unlikely that such an agency will effectively implement a policy which affects every U.S. employer. Clearly, implementation of sanctions thus far, and the lack of promise that the law can ever be implemented effectively, are much more responsible for the weakness of the policy than the lack of a national identifier.

---

[12] Select Commission op.cit.

[13] Wayne A. Cornelius. "Presentation to the Ninth Annual Briefing Session for Journalists," Center for U.S.-Mexican Studies, June 22, 1989.

[14] Robert L. Bach and Howard Brill, "Shifting the Burden: The Impacts of IRCA on U.S. Labor Markets," State University of New York, February 1990.

[15] "Four Years After Reform," *The Government Executive*, September 1990.

[16] Unfinished Business, op.cit.

[17] Michael Fix and Paul T. Hill, Enforcing Employer Sanctions: Challenges and Strategies, (Rand Corporation, Urban Institute), May 1990.

B. National ID system not likely to be effective

Even if Congress were to ignore the many fatal flaws inherent in employer sanctions and move to implement a national ID system using the social security number, there are strong reasons to doubt that such a system would increase the effectiveness of employer sanctions in curtailing illegal immigration. Presumably, the ID card is being proposed because of the fear that undocumented workers are responding to employer sanctions by obtaining fraudulent documents. The simple establishment of a card, however, is not a guarantee that a market for false papers, if it exists, will be eliminated. As mentioned above, just as the discriminatory scrutiny of documents is likely to be transferred to the process of obtaining underlying documents under a new ID system, so is the process of obtaining fraudulent documents. A national ID system can only be secure if accompanied by methods of ensuring the security of all documents which establish identity, residence, and work authorization; however, such a comprehensive policy is likely to be excessively costly, both in monetary terms and in terms of human and civil rights.

Even if Congress were to choose a comprehensive identification policy which involves a large array of documents, current experience with employer sanctions suggests that such methods do not discourage undocumented immigration, but rather push the undocumented further underground. The first attempt by the United States to eliminate a large class of unauthorized workers, the end of the notorious *bracero* program, did not succeed in its goals, and instead paved the way for the foundation of what is now a sizeable undocumented community living and working within the U.S. According to immigration scholars Alejandro Portes and Ruben Rumbaut, the 1964 termination of the *bracero* program "was prompted by the desire to curtail low-wage foreign labor; instead, this Mexican labor inflow went underground and then expanded rapidly."[19] There is ample evidence indicating that employer sanctions have had the same effect; rather than curtailing undocumented immigration, they have pushed undocumented immigrants underground, subjecting them to poor wages and working conditions.[20] The failure of the Latin Investment Company in Washington D.C. provides a recent example of how, when faced with increasing restrictions, undocumented immigrants simply begin to function in a underground economy, making them subject to greater levels of exploitation. All of the evidence surrounding employer sanctions suggests that "strengthening" the policy by even the most comprehensive documentation system will simply push people further underground; thus, a policy intended to prevent exploitation will actually provide more avenues for it to occur.

C. Logistical problems with a national ID system

Perhaps the most glaring threat to the successful implementation of a national ID system are the data-management problems within the INS. Clearly, for a national identifier to be used in the immigration context, it will have to be tied in somehow to information from the INS which verifies immigrant status or work eligibility. One such verification program, the Systematic Alien Verification for Entitlements (SAVE) program, is already in operation in the hope that it will prevent ineligible aliens from receiving public benefits. A 1987 study by the General

---

[18] Unfinished Business, op.cit. pp. 31-32.

[19] Alejandro Portes and Ruben G. Rumbaut, Immigrant America: A Portrait, (University of California), 1990, pp. 234-235.

[20] Unfinished Business, op.cit.

Accounting Office (GAO) shows that "there is considerable room improving the accuracy and reliability of the automated system."[21] According to the GAO, 30.5% of the individuals applying for verification needed a secondary check, because their information could not be found in the data base. Secondary checks, which are performed manually, are both costly and time consuming. In the case of SAVE, such aliens continue to receive benefits unless they are ultimately proved to be ineligible; under a work authorization card system, delays for secondary checks could cost work-authorized immigrants their jobs.

In addition, there is substantial evidence that INS data management is not up to the task of integration with a national ID system. A recent GAO study of INS information management highlights severe problems, including inaccurate information, inadequate data verification, data entry backlogs, missing case files, and inadequate user training.[22] This, as well as a recent draft management study by the GAO confirm what those of us who work with the INS have known for decades; that there are enormous bureaucratic problems within the agency which frequently prevent it from effectively performing its duties.[23] In this case, adopting a national verification system will mean that the job opportunities of literally millions of "foreign looking" persons will hinge on the ability of the INS to produce accurate data quickly. This is simply unacceptable from every standpoint.

V. CONCLUSION

Perhaps more important than any of the above arguments, the notion of "fixing" a clearly discriminatory policy with an untried and probably equally troublesome new system is offensive to those of us who warned the Congress that employer sanctions was an unworkable and dangerous public policy. NCLR sat before the immigration subcommittees in the House and Senate numerous times and predicted that sanctions would not prove to be effective, and that they would cause enormous levels of discrimination. Our objections to the policy were not heeded, and the promise that the policy would be repealed if it proved to be discriminatory has been broken. Congress has not kept faith with the Hispanic and Asian communities, even though our direst predictions have proved to be true. We are alarmed that Congress again appears to be considering a dangerous new policy initiative which we are again certain will damage the fundamental rights of our community. Last year such a proposal nearly passed over our objections. NCLR urges this Subcommittee to reject any proposal for using the social security number or any other system as a national identifier. We particularly object to such a proposal emerging in the immigration context. We further urge that the Subcommittee exercise great vigilance; proponents of such a proposal have already attempted to force it through without proper consideration. The prospect of a national ID system as an supplement to employer sanctions presents little likelihood of repairing a fundamentally flawed policy, and is enormously dangerous to communities whose rights are already being violated in the name of immigration control.

---

[21] Immigration Reform: Systematic Alien Verification System Could Be Improved, U.S. General Accounting Office, September, 1987.

[22] U.S. General Accounting Office, Information Management: Immigration Service Lacks Ready Access to Essential Data, September, 1990, p. 5.

[23] U.S. General Accounting Office, "Immigration Management: Strong Leadership and Management Reforms Needed to Address Serious Problems," Draft Report.

Chairman Jacobs. Thank you, Ms. Munoz.
Mr. Simcox.

STATEMENT OF DAVID SIMCOX, DIRECTOR, CENTER FOR IMMIGRATION STUDIES

Mr. Simcox. Thank you, Mr. Chairman.

I thank you for the opportunity to appear before this committee on the complex question of the appropriate use of the Social Security number as a national identifier. I don't recall that the issue of the national ID card was specifically posited in your proposal. As the second to the last witness, and the last session I will shorten my remarks to what I perceive to be the general level of attention prevailing in this room.

My center, the Center for Immigration Studies is a nonprofit research and policy analysis group that examines the options for humane and effective enforcement of our immigration laws in ways consistent with democratic values. Our studies have dealt with the appropriate use of nonintrusive security ID systems in support of such objectives as implementation of employer sanctions, the screening of nonentitled aliens from public assistance rolls and the Federal firearms legislation that bars illegal aliens and persons who have lost their U.S. citizenship from gun ownership.

Mr. Chairman, I will probably not be the only witness that will appear before you, in your tenure in this position, to assert that this country's loose and decentralized system of personal identification remains an open invitation to massive fraud and abuse and a serious impediment to serious law enforcement. No case is more the case than in the enforcement of immigration laws. And I would also add as a personal note my feeling that the country's weak identification standards, in themselves, constitute a standing threat to an important privacy right. The right of all of us, citizens and illegal aliens, to be protected against the misappropriation of our identities.

This anarchic situation was amply documented by the Federal Advisory Committee on False Identification in 1976. Since that time, Congress has enacted numerous laws that attempt to tighten ID standards or which depend, in themselves, on improved identification security for their effectiveness. Even so, 15 years after the Federal Advisory Commission, the security of personal identification in the United States remains among the worst in the western world.

No Federal law enforcement effort has been more hampered by document fraud than employer sanctions. Pervasive counterfeit or alterations of documents purporting to establish work authorization are seriously undermining the deterrent effects intended by Congress in the 1986 IRCA. The sharp rise in alien apprehensions in 1990, after 3 years of decline suggests that those considering illegal entry into the American labor market now are convinced that employer sanctions are easily evaded. And general respect for all our laws are suffering in the process.

The diversity and unreliability of the 17 different categories of documents authorized as proofs of identity and work eligibility is fatally confusing to workers and employers, as well as enforcement officials and are a standing invitation to abuse. This jumble of documents has placed otherwise well-intentioned employers in a dilemma. Many have responded by accepting suspect documents, no questions asked. While others have unintentionally discriminated against job seekers by insisting on certain documents they feel are generally more reliable.

Mr. Chairman, it is time to accept that the existing arrangements for documenting identification and work eligibility simply does not work and to move on to more secure systems that were envisaged by the 1986 law. The language of that legislation should suggest doubt on Congress' part that the existing system of documents would do the job and others would have to be considered.

The prudent use of the Social Security number, validated by the Social Security Administration can greatly help in making basic ID documents more fraud-proof and establishing effective verification systems without violating legitimate privacy concerns or seriously increasing administrative costs.

If we are to end unauthorized employment, ease the paperwork burden on the Nation's 7 million employers and banish job discrimination we should move toward a universal call-in system based on the Social Security number to verify the nearly 60 million hiring transactions that take place in the U.S. economy each year.

The increased administrative cost of such a system would be offset by the reduced need for workplace enforcement measures and the ultimate elimination of the burdensome I–9 verification form, and lower FICA tax evasion. The Social Security Administration, itself, would gain from it by cleaning its records of numbers now being used by more than one person or by impostors.

I recognize and it is doubly confirmed by what I have heard today that political privacy and budgetary concerns will work against early creation of such a universal system. But Congress should authorize pilot projects for Justice and HHS to work together in developing the concept.

Until that time, there are two feasible interim measures that will help preserve the credibility of IRCA and enhance the country's ID standards. INS should be authorized without further delay to begin its pilot project for a phone-in system for verifying worker eligibility.

Chairman Jacobs. We will include the rest of your statement in the record, Mr. Simcox.

Mr. Simcox. Thank you, Mr. Chairman.

[The prepared statement follows:]

TESTIMONY OF DAVID SIMCOX
CENTER FOR IMMIGRATION STUDIES

Mr. Chairman:

I am happy to have the chance to appear today before this committee on the complex question of the proper use of the social security account number as a national identifier. The Center for Immigration Studies, which I head, is a non-profit research and policy analysis group, one of whose objectives is to examine the options for humane and effective enforcement of our immigration laws in ways consistent with democratic values. Central to this undertaking is consideration of the appropriate use of non-intrusive secure identification systems in support of such legislated objectives as enforcement of employer sanctions, the screening of non-entitled aliens from public assistance rolls, and federal prohibitions on the ownership of firearms by illegal aliens and persons who have lost their U. S. citizenship.

The appropriate balance among the imperatives of security, efficiency and privacy of national identification systems is a question now facing other western industrial nations along with the United States. Recognizing the transnational character of this issue, the Center for Immigration Studies sponsored in November of 1990 an international conference of identification and privacy experts from thirteen industrial nations, including the Soviet Union and Japan. Discussions ranged over such issues as the appropriate purposes and safeguards for national identification numbers; special purpose identification numbers such as those for tax, social insurance, voter registration and property ownership; national identification cards for citizens and aliens; and national population registers. The conference also addressed safeguards for the security and privacy of vital records.

An important issue at the conference was the nature and extent of the threat of abuses of privacy from national ID numbers, or from special purpose numbers now broadly used, such as the U. S. social security number and Canada's social insurance number (SIN), because of their facilitation of computer matching. There was general agreement that special use numbers covering broad populations become a valuable public administration resource that tend to invite use for purposes not originally unintended. But representatives of the Western European continental democracies showed greater pragmatism than the U. S. and other common law countries (U. K., Australia and Canada) in accepting the public administration advantages of such systems. Moreover, unlike the United States, nearly all Western European countries have the extra protection of centralized, semi-autonomous data protection agencies or privacy commissions to guard against abuses of ID numbers and related data, backed up by legislation based on international privacy standards.

There was considerable discussion of whether ID numbers do in fact facilitate the matching of data to a dangerous degree. The assumptions underlying that proposition were questioned. It was noted that the existence of ID numbers as identifiers is no longer a necessary condition for efficient matching of personal data; in any event, unauthorized matching is best discouraged by means other than the imposition of "inefficient identifiers."

Evidence was presented showing that highly efficient matching is possible without ID numbers, using such identifiers as names and birth dates -- an efficiency that steadily improves with advances in computer technology. The second questionable assumption -- that technical self-limitation is an effective safeguard -- is particularly applicable to the U. S. experience. As Norwegian delegate Knut Selmer expressed it:

> "The defense of democratic values must be sought elsewhere. The suppression of birth numbers or other technical means will only postpone the troubles; technical obstacles could always be circumvented. There

> must, in other words, be a constant awareness in political circles that data technology can endanger our democratic values. Furthermore, there must be potent public organs with the single task of supervising the use of computers in the administration, and sounding the bell if the development gives rise to anxiety (Selmer, 1990)."

I share this view. The massive collections of data now held by Federal and state agencies and managed with the most sophisticated data processing techniques can be seen as a rich resource rather than as Leviathan, not as a threat but as an opportunity for highly efficient public administration and provision of services that improve our quality of life, our protection from crime and abuse, and even our privacy. Self-imposed inefficiencies in the management of such a resource as a protection against abuse is wasteful and ultimately self-defeating. An enlightened democratic society is capable of devising far better and more flexible safeguards.

Identification Anarchy Undercuts Immigration Control

It is hardly news that this country's diverse and decentralized non-system of personal identification is what the Reverend Theodore Hesburgh called "anarchic," an open invitation to massive fraud and abuse and a serious impediment to effective law enforcement, including compliance with the immigration laws. Such a system also entails its own unique threats to individual privacy. The Federal Advisory Committee on False Identification (FACFI) amply documented this broad pattern of abuse in its 1976 report. While the situation has improved little since the mid-1970s, Congress has since approved a series of laws that demand better identification for their effective enforcement or which increase the penalties on those engaging in abuses of documents. Congress in the 1984 Omnibus Crime Control Act required Federal agencies to move toward greater commonality in their own identification systems and directed the Executive Branch to submit recommendations for secure federal identification systems by 1987. Unfortunately the Executive has ignored this Congressional instruction.

No federal enforcement effort has been more hampered by document fraud than sanctions against those who employ unauthorized aliens. Pervasive and easily available counterfeit documents purporting to establish work authorization are seriously undermining the deterrent effect of the 1986 immigration reforms, eroding basic respect for the law in general. The resurgence of illegal immigration in 1990, as indicated by a sharp rise in apprehensions of illegal aliens after three years of decline, suggests that once hesitant candidates for illegal entry into the American workplace are now convinced that employer sanctions are easily evaded.

Looking at the diversity and unreliability of the crazy quilt of documents authorized by the Immigration and Naturalization Service (INS) to prove identity and/or work eligibility, it's hard to see how enforcement of sanctions could be anything but confused --for employers and workers as well as enforcement officials. INS originally designated 17 different documents as acceptable for use. But a number of the acceptable documents are in themselves broad categories of diverse documents of varying quality and reliability, further taxing the employer's ability to judge authenticity among so many different permutations.

Some examples:

o Drivers licenses, issued with different formats, security standards and personal data by 50 states and five other jurisdictions.

o Baptismal records, issued without uniform standards or formats by nearly 100,000 parish churches that practice infant baptism.

o Social Security cards, with more than 15 versions in use, and only the most recent with any counterfeit-resistant features.

o Voter registration cards, issued in different formats by the 50 states, often by mail with no confirmation of identity or legal residence status.

o INS "green cards," with three versions in use, two of them readily counterfeitable.

o A basic breeder document for other ID, the birth certificate is issued by some 7000 different jurisdictions, with widely varying formats and security arrangements.

Besides undermining enforcement, this jumble of easily abused documents has placed otherwise well-intentioned employers in a dilemma: many have responded by accepting suspect documents "no questions asked;" while others have unintentionally discriminated by insisting on specific documents of presumably greater reliability from job seekers.

Options for Better Verification: A Social Security Call-in System

So the identification arrangements set in place since the 1986 IRCA have clearly failed. Now is the time to move to more secure systems as that law envisaged. But while the responsible agencies have completed the mandated studies of the options for telephone-in systems, secure social security cards, and employer validation of the social security numbers of job candidates, there has been little movement toward actual choice and implementation of alternative systems in the nearly five years since IRCA.

INS has been stalled for nearly three years in getting the go-ahead for a pilot project to test a phone-in system of verification. The system to be tested is at best is modest in scope and only partially responsive to broad enforcement needs. It will provide verification only to those job seekers who are -- or who admit to be -- foreign born and it relies on a data base keyed to the Alien ID number or "A-number," rather than the social security number.

Legislation failed in the last Congress to authorize a limited pilot project in a few states to examine enhanced security features, including biometric identifiers and personal data, that would make the drivers license or non-drivers state identification card a key document in worker verification.

Mr. Chairman, I believe that prudent use of the social security number can greatly contribute to current efforts to make basic ID documents more fraud proof and establish effective verification systems, without violating legitimate privacy concerns or loading major uncompensated administrative costs on the government.

Over the longer term, if the burdens and perplexities of the nation's seven million employers are to be eased, IRCA-related job discrimination banished, and unauthorized employment ended, it will be necessary to move to a universal call-in system (using phone, modem or point of sale device) based on the social security number that would verify the 50 to 60 million hiring transactions that occur in the U. S. economy each year. While such a system would entail added administrative costs, these would be offset by reduced costs of workplace investigations and other on-site enforcement measures that would be obviated.

The amount of individual data on nearly 250 million social security enrollees required for such a verification system should be limited to the minimum required to establish positive identification. The data base containing it should be administered separately from the main files of the Social Security Administration. If a transaction number were provided to employers for each phone-in verification, the employer would have a record of compliance, ultimately making it possible to dispense with the burdensome I-9 verification form.

There would be other administrative benefits as well. Verification of job applicants against social security account data would aid in ridding the system of invalid or inactive numbers and in controlling use of numbers by more than one person or by impostors. Avoidance of FICA taxes would be reduced.

I recognize that political, privacy and budgetary concerns work against early creation of such a universal system. But Congress should authorize pilot projects involving the Departments of Justice and Health and Human Services to further refine the concept and draw on the experience of other on-going projects for enhancing ID systems.

Near Term Improvements: A Call-in System and Secure Drivers Licenses

In the interim, the following measures, more politically and administratively feasible, would help restore the credibility of IRCA and enhance the general quality of identification in the country, most of them involving use of the unique resource of the social security number:

o The INS should begin without delay the pilot project for phone-in verification of worker eligibility, testing it among a variety of employers and conditions. Reliance on the "A-number" in the INS data bank, the "Central Index", entails serious limitations and will impede the ultimate evolution of a far more efficient, universal system based on social security numbers. But as an interim measure, all individual files in the INS central index should contain the alien's social security number as well as "A-number", appropriately validated by the Social Security Administration.

o Congress promptly should authorize a pilot project to work with interested states in developing a uniform drivers license and state ID card secured by a biometric identifier, such as a digitized fingerprint or photograph, and by a social security number of the bearer pre-validated by the Social Security Administration. The project should build on the innovations for data storage in the new California drivers license, moving ultimately to the use of "smart cards." The drivers license could be appropriately coded for use in employment transactions in proving both identity and eligibility to work in the U. S. A simple binary code would specify either that the bearer was unconditionally eligible to work in the U. S., or that the document was valid for work eligibility only when presented in conjunction with a suitable INS document. Personal data on individual drivers would remain under the control of the license issuing states, but available for rapid exchange among the states upon legitimate request through a central clearing house.

The existence of numerous models, precedents and preparatory studies would permit rapid progress toward secured licenses and non-driver ID cards for the nation's nearly 180 million users. The Commercial Drivers Licensing System (CDLIS) now serves as the model for secure licenses using biometrics. Covering five million truck and bus operators, CIDLIS has a central clearing house for sharing of data among the states to prevent multiple licensing and track problem drivers.

The Social Security Number now is used for drivers licenses by 41 states. In its 1998 report to Congress on the feasibility of a system of employer validation of social security number, the Social Security Administration counterproposed a system of pre-validating social security numbers on licenses for the states. With costs and political considerations impeding the development of a secure social security card, the secure drivers license or state ID card with a pre-validated social security number would become a useful surrogate in transactions where confirmation of the social security number is needed. The states would also thus be positioned to ensure the integrity of the voter rolls if Congress were to enact "Motor-Voter" legislation as originally considered in the 101st Congress.

Finally, the concept of pre-validation of social security numbers should be considered for use in other vulnerable identification systems, such as passports issued by the Department of State. The machine-readable personal data page of the U. S. passport, with pre-validated social security number and a biometric identifier, and with secure lamination and other tamper-proof features, could be produced and sold to passport holders as a secure, voluntary ID card. Such cards, uncontestable evidence of identity and work eligibility, could be an important revenue raiser and an alternative document for travel within North America and Western Europe.

Thank you.

Chairman JACOBS. Mr. Stein.

STATEMENT OF DANIEL A. STEIN, EXECUTIVE DIRECTOR, FEDERATION FOR AMERICAN IMMIGRATION REFORM (FAIR)

Mr. STEIN. Thank you, Mr. Chairman.

My name is Dan Stein and I am executive director of FAIR. I appreciate the opportunity to be here. I commend you, Mr. Chairman, for holding this hearing.

FAIR is an organization working nationally to bring about reasonable balanced approaches to controlling illegal immigration and enforcing legal immigration laws. Mr. Chairman, I have with me, here today, literally thousands here and in the back of the room, of different types of fraudulent documents, courtesy of the Department of Justice. I have Social Security cards, both blank and fraudulent; registration receipt cards for aliens; certificates of naturalization; Illinois voter registration cards; Selective Service cards; records of arrival and departure; resident alien cards; State of Texas birth registration cards. I even have a State of Indiana achievement test certificate.

Chairman JACOBS. Can I have that? [Laughter.]

Mr. STEIN. That probably doesn't surprise you but it points out that we are really talking about two different issues in this hearing. One is the use in the private sector of the Social Security card to circulate private information about people. The second one is linking the Social Security card to the people to whom it was originally issued.

Mr. Chairman, we are concerned because the world is changing. As Abe Lincoln said "When our situation is new we must think and act anew." We are adding about a billion people to the planet every 10 years in the world today. In fiscal year 1989 there were 434 million total inspections across our land borders of entry. This is a total increase of 42 percent since 1984. There were 864 inadmissible aliens detected at all of those ports of entry. And illegal immigration is a serious problem. Last year alone, 1.169 million illegal aliens were apprehended at the borders of the country crossing illegally.

Now, in 1986, Congress concluded that illegal immigration was a serious national problem. It enacted employer sanctions as the corner stone of a national program to curtail the employment of illegal aliens. Employer sanctions are working but they are being undermined by the flourishing and confusing array of documents that can be bought and used, and that have made it very difficult to verify who is here and who is not.

No one who originally supported employer sanctions ever believed that relying on this existing panoply of documents that are accessible under the I-9 for employers could ever be effective in the long-run. The 1986 act gave the executive branch a clear directive to propose to Congress explicit, new provisions for developing a better document verification scheme. The executive branch virtually ignored that directive.

So we are back here now trying to push the second half of this program and what Senator Simpson is trying to do is to push this to completion. We are advocating the establishment of secure, uniform work verification system to simply ensure that the Social Security number which is presented and required by law to the employer is, in fact, the number that was originally and legally given to that person. This system would use one document, the Social Security card, or one number, don't even need the document, the number, itself, which could be verified through a telephone verification system. And verification would be based on data already in the Social Security files and already used for a variety of purposes, identifying numbers on driver's licenses and tax returns.

This verification procedure would be triggered when an individual applies for a job. And would be applied to every job applicant regardless of citizenship status. And the system would be legally constrained by the Privacy Act of 1974, as well as the privacy considerations contained in IRCA.

Now, the Roper organization did a poll in June of 1990 which found that 62 percent of Americans, including Hispanic Americans supported the use of an electronically verifiable or machine readable Social Security verification scheme at the time of hire. So there is overwhelming public support for that. And requiring the Social Security Administration to verify that a prospective employee is using a valid Social Security number is not an expansion of their current mission. Preventing the use of false numbers is an essential part, or should be an essential part of their mission. An employee who furnishes a wrong number by mistake may lose benefits that he has earned. An employee may also furnish false numbers to evade Federal income taxes.

Critics who say that a secure means of determining the validity of a prospective employee's Social Security number is an erosion of civil liberties are attacking not only employer sanctions, but also our income tax withholding and Social Security programs, since the furnishing of a valid Social Security number is essential to those systems, as well.

Why do we have all of these phony documents when we have a single number circulating through all of these private data bases? The answer is and we can never forget this issue is that the Social Security number is built on a foundation of sand because we do not have an accurate means of determining who was born in this country and who was not. As more and more people come into this country illegally and affect legal jurisdiction, it is becoming increasingly difficult to effectively identify and deport people who come illegally. Getting a handle on this issue is essential to regaining control of our borders and I urge this committee to take a serious look at Senator Simpson's proposal in this Congress.

Thank you, Mr. Chairman.

[The prepared statement follows:]

TESTIMONY OF DANIEL A. STEIN
FEDERATION FOR AMERICAN IMMIGRATION REFORM

THE NEED FOR A SECURE UNIFORM WORK VERIFICATION SYSTEM

Mr. Chairman and members of the committee, thank you very much for the opportunity to appear on behalf of the Federation for American Immigration Reform (FAIR). My name is Dan Stein and I am the executive director of FAIR. FAIR is a national non-profit, public interest organization working to end illegal immigration and to set legal immigration at levels consistent with the realities of the 1990s.

My testimony today is about the need to establish the secure uniform work verification system mandated by Congress four years ago in the Immigration Reform and Control Act. P.L. 99-603, codified at 8 U.S.C. 1324a, et seq. (1986).

1. The Problem: Illegal Immigration

Illegal immigration is a serious problem in the United States. Last year alone 1,169,939 illegal aliens were apprehended at the borders of this country. The Immigration and Naturalization Service (INS) estimates that for every one illegal alien the Border Patrol apprehends, another two or three cross the border. (This figure, however, is the low estimate; the INS high estimate is that for every one illegal alien apprehended, five to seven cross the border.) In 1989, the last year for which figures are available, there were approximately two to three million illegal aliens residing in the United States.

In 1986, after more that ten years of debate, Congress finally passed the Immigration Reform and Control Act (IRCA). One of the most significant components of this landmark legislation was the employer sanctions provision which prescribed penalties against employers who knowingly hire illegal aliens.

In order to protect both the persons subject to penalties and the members of minority groups legally in this country, IRCA provided a system to verify that employees and potential employees are eligible to work in the United States. To prove identity to an employer, an individual may submit any of 21 documents, including a driver's license or a voter registration card. To prove employment eligibility, any of 17 documents, such as a Social Security card or birth certificate, are specifically authorized under the law. (Typically, the documents used are a driver's license for identity, and a Social Security card for eligibility). To comply with the law, the employer must certify that he/she has reviewed the documents and that "they appear genuine" and relate to the applicant.

2. The Solution: IRCA

a. Unfulfilled Mandates

IRCA required the General Accounting Office (GAO) to conduct three annual studies to review the implementation and enforcement of employer sanctions for the purposes of determining if the law: (1) has been carried out satisfactorily; (2) has caused widespread discrimination to eligible workers solely due to sanctions; and/or (3) has caused an unnecessary burden on employers. 8 U.S.C. 1324a(j)(1986).

All three reports have been completed and all three reports indicate that IRCA has reduced illegal immigration. In the third report, released in March, 1990, the GAO found that IRCA was not a burden on the nation's employers and recommended that employer sanctions be retained and strengthened. Although the report indicated that a small amount of unlawful discrimination against workers did occur, the GAO was unable to determine whether any of the discrimination they uncovered was against eligible workers, or against ineligible illegal workers.

What was clear from the third report was that nearly all the cases of alleged discrimination had resulted from employer confusion about the types of documentation they may accept as proof of work eligibility. Thus, a uniform system, which IRCA's drafters advocated and provided for in 1986, combined with employer sanctions and increased manpower along the border, would both significantly reduce the flow of illegal aliens into the United States and insure against potential sanctions-related discrimination.

In its March 1990, report entitled, "Employer Sanctions and the Question of Discrimination," the GAO recommended a "fundamental reform" of the current verification system which could be accomplished simply by complying with IRCA's provisions. The report noted that the provisions of Section 101(a)(1) of IRCA, which specifies that any improvement to the verification system should yield reliable determinations of employment eligibility and identity, be counterfeit-resistant, be used for employment verification only, protect individual privacy, and not be used for law enforcement purposes unrelated to IRCA,

> are consistent with the types of changes we believe are necessary to the verification system to reduce discrimination. Increased reliability would make it easier for employers to comply with the law. Counterfeit-resistance would increase employer confidence that documents being presented were genuine. Privacy guarantees and prohibitions against using the employment verification system for other uses would reduce fears among both employers and prospective employees of unjustified government intrusion into their lives. Thus, when combined with fewer work eligibility documents and universal application throughout the work-force, such improvements to the verification system should both reduce discrimination and increase the effectiveness of sanctions.

General Accounting Office, "Employer Sanctions and the Question of Discrimination" (1990).

There is a great deal of public support for a uniform, secure work verification system. In a poll conducted in June, 1990, by the Roper Organization, concerning "American Attitudes Toward Immigration," 62% of those questioned stated that they favored a government-issued, forge-proof, easily verifiable identification document that would have to be shown only when applying for a job.

Employer sanctions will never be as effective as they were meant to be until all of IRCA's provisions are fully implemented. That is why I am at a loss to explain why the United States Congress and the president have not seen to it that IRCA's mandates, so clearly spelled out four years ago, have been implemented and enforced. Is this failure to follow through a bureaucratic oversight or a deliberate attempt to undermine IRCA's employer sanctions provisions? Of course, although neither reason provides a legitimate excuse, a deliberate attempt to program for failure what has been the law of the land for the past four years is much more serious and, in fact, suggests that these two branches have a somewhat hypocritical approach to governing. If the government is going to refuse to comply with its own laws, why should average citizens be expected to obey the law? Or, is that the point? By ignoring IRCA's mandates, are Congress and the president admitting that they are not opposed to illegal immigration? By not doing everything they can to ensure IRCA's success, are Congress and the president actually encouraging illegal immigration?

IRCA came about because of widespread concern on the part of average citizens, i.e., constituents, about illegal immigration, and the perception that it was out-of-control. Many Congresses and many compromises would pass, however, before these concerns were put into law. The most important, and controversial, compromise in IRCA required trading amnesty for employer sanctions. This amnesty, which legalized 3.1 million illegal aliens, has already been implemented and cannot be revoked; the employer sanctions provisions continue to struggle under the weight of unfulfilled directives and unrelenting repeal efforts.

b. Following Through With the Studies Required by IRCA

IRCA mandated that a number of studies be conducted relative to the verification of employment eligibility: (1) Three annual presidential reports on the employment verification system (to be issued after the first year of implementation). Each report is to analyse the system's adequacy and describe the development and implementation of changes to the system; (2) A report by the Attorney General on the potential use of a telephone verification program for determining the employment eligibility of aliens; and (3) A study by the Secretary of Health and Human Services on the feasibility and cost of a Social Security number validation system to help employers comply with IRCA.

(1) Presidential Reports

In October 1990, the Justice Department announced that it will seek, this year, a delegation to the attorney general of the president's authority under section 274A of the Immigration and Nationality Act (INA), so that the INS can conduct demonstration projects to evaluate the effectiveness and security of the employment verification system required by IRCA, and be able to recommend or implement such changes as are necessary to establish a more secure system.

Section 274A(d) directs that "[t]he President shall provide for the monitoring and evaluation of the degree to which the employment verification system established under subsection (b) provides a secure system to determine employment eligibility in the United States and shall examine the suitability of existing federal and state identification systems for use for this purpose. To the extent that the system established under subsection (b) is found not to be a secure system to determine employment eligibility in the United States, the President shall . . . implement such changes as may be necessary to establish a secure system to determine employment eligibility in the United States."

(2) Telephone Verification

IRCA provided authorization for the president to request the attorney general to test telephone verification as an alternative to physically presenting documents to employers during hiring transactions. Patterned after credit card systems, it would enable employers to transmit electronically a number, perhaps the social security number, to receive verification of work eligibility.

In its March 1988, report entitled "A New Role for the Social Security Card," the GAO described a pilot project conducted by the Social Security Administration (SSA) in 1987, to determine the feasibility of a telephone verification system for the use of employers. The project's goals were to (1) evaluate ways to more effectively control the issuance of Social Security numbers and their use in the workplace, and (2) reduce the incidence of earnings reported by employers for their employees under incorrect Social Security numbers. Also, the study was designed to help the SSA prepare for the Social Security number validation study required under IRCA.

Participation in the project, begun January 20, 1987, was voluntary and available to about 70,000 employers in the Dallas, El Paso and Corpus Christi areas. By the end of the year, employers made about 13,500 calls to verify 23,158 social security numbers of prospective employees. The SSA was able to verify 81% of the numbers provided for verification. A name mismatch was the primary reason numbers could not be verified. Other reasons included: the date of birth differed, the number provided was invalid, or the individual was not authorized to work.

Although successful where it was conducted, it is not clear whether this pilot program can accurately project the results of a national verification project because it was limited in several ways: it was voluntary; the three cities selected were in an area with a large illegal alien population, which could skew the results of verifications attempted; and the employers' calls were handled manually, rather than with an automated system. Nevertheless, the GAO concluded that the project is important because it "provided some assurance to employers that the Social Security card presented by prospective employees was valid and the individual presenting it was the owner. This verification could reduce the number of individuals using fraudulent cards with invalid numbers, non-work or restricted Social Security cards, and cards belonging to children or other persons where the age entered differs significantly from that of the bearer of the card."

Of course, implementation of telephone verification would require the INS to upgrade dramatically the attention and professionalism accorded its record-keeping systems. Records responsibilities have been chronically neglected by the agency, and records security is often haphazard. A 1989 audit showed about 17% of the data from its central alien information repository to be missing or incorrect.

(3) The Social Security Card

Under IRCA, the nation's estimated 7 million employers are required to review thousands of different documents allowed as evidence of identity and employment eligibility. Most employers, however, are not in a position to make sound judgments on the genuineness of these documents. Indeed, employers have been given little guidance and education on the characteristics of fraudulent and genuine documents. Morever, even SSA employees, who are trained in document authentication, often have difficulty determining whether documents are authentic and relate to the person presenting them.

Originally, the Social Security number (SSN) had a single use -- to keep track of an individual's earnings so that Social Security retirement eligibility could be verified and an accurate benefit amount computed. Today, however, the number has a wide variety of uses, for example, as an identifying number on drivers' licenses and tax returns. About 330 million numbers have been issued, 210 million of which are considered active. There are 16 versions of the card in use. Until 1972, the SSA issued cards without requiring evidence of identity, age, or citizenship. Now, however, such evidence is required, and birth certificates are commonly accepted in support of an application for a card.

To improve employer verification under IRCA, the SSN card should be designated as the only authorized employment eligibility document. Such an option should have minimal adverse impact on the public: The IRS already requires that all employees have an SSN for tax purposes.

The GAO supports the use of the SSN card as the only document that can be used as evidence of employment eligibility under IRCA. In a March 1988, report, the GAO stated that

> [w]e believe that the [SSN] card would meet the needs of both employers and employees and offer advantages over the present system.
>
> With such a change, employers would have only the [SSN] card with which to become familiar, rather than the thousands of different birth certificates and other documents that now can be provided as evidence of employment eligibility. Also, educating employers in detecting fraudulent cards would be more feasible than trying to educate them on the many types of documents now authorized.

General Accounting Office, "A New Role for the Social Security Card" (1988).

In its IRCA-mandated report regarding SSN validation systems, the Secretary of Health and Human Services proposed using state drivers' licenses as a method for validating employment eligibility. The report found that 29 states issue licenses showing the SSN; some request verification of the number from the SSA at the time of issuance. In these latter states, license holders are, in a sense, pre-validated for work purposes because the photo on the license links the SSN to the job applicant when presented to an employer.

A recent report by the Center for Immigration Studies noted that use of drivers' licenses to verify employment has a number of advantages. For example, the report pointed out that

> the issuance of driver's licenses is decentralized among the fifty states and several territories, avoiding the coloration of a centralized 'big brother'apparatus. . . . Although decentralized, [this] system has developed effective methods and organizations for exchanging information quickly, such as the National Drivers Register, with some 8 million records of problem drivers, and the Commercial Drivers License Information System (CDLIS), which will ultimately track information on 5 million truck and bus operators.

The Center for Immigration Studies, "Secure Identification: A National Need -- A Must for Immigration Control" (1990).

3. Cost and Privacy Concerns

Critics of a secure uniform work verification system claim that it would be too costly and that it would pose a threat to privacy.

a. Costs

Since 1986, the GAO has conducted several studies on the adverse effects of illegal immigration. These studies have included the displacement of U.S. workers (April 1986), the cost of uncompensated health care (September 1987), criminal alien activity in the U.S. (November 1987), the amount of governmental remittances sent back to foreign countries (February 1988), the influence on wages and working conditions of legal workers (March 1988), and the existence of sweatshop conditions in the U.S.

(August 1988), just to name a few.

What the GAO discovered is that illegal immigration costs federal, state and local taxpayers, combined, billions of dollars annually. For example, the GAO found substantial evidence that illegal aliens displace (take jobs away from) legal workers. The result of this, of course, is increased worker dependency on federal unemployment and welfare benefits. In fact, the Congressional Budget Office (CBO) estimates that each unemployed person in the United States receives an average of about $7000 per year in these benefits. If the number of illegal aliens in this country today is estimated at 3 million and if even 1% hold jobs which unemployed Americans would take, then the savings would be $210 million per year; if the displacement is 2%, the figure would be $420 million per year, etc. Actual displacement is probably substantially higher.

The GAO also found that illegal aliens use hundreds of millions of dollars each year in unreimbursed health care. In Los Angeles County alone, the Department of Health Services has spent over $768 million in the past five years for unreimbursed health care to illegal aliens. This does not include costs for bilingual education, welfare benefits or other social expenditures.

Public schools are the hardest hit. For example, in 1989, school officials in Dade County, Florida, estimated that, in order to keep up with the incoming flow of illegal aliens, they would need to hire two new teachers each day and build one new school each month.

How do these costs compare to those involved in establishing a secure uniform work authorization system? The SSA has estimated that the cost of replacing all SSN cards with a tamper- and counterfeit-resistant version would be $108 million a year for 10 years. The actual cost of this option should be lower since replacement of all cards would not be necessary. (The GAO has suggested that an option for financing the cost of replacement SSN cards would be to charge a fee for all or certain replacements.) The Department of Labor has estimated the cost of a verification system utilizing telephone calls to a government data bank as averaging $333 million per year for the first 5 years and about $200 million per year thereafter. Doubling the number of interior INS investigators would add $25 - $30 million per year. Thus, a new system to verify work eligibility clearly will not exceed in cost the amount directly saved as a result of reduced public assistance alone, not even considering the value of the other benefits of reducing illegal immigration.

b. Civil Liberties Issues

The business of governing is never easy. There is no textbook to consult, no hard and fast set of rules to systematically follow. The paramount objective, of course, is to govern in such a way that the greatest number of citizens benefit from, or at least are not harmed by, the results. This involves a balancing of competing and, often, contradictory interests. To be effective, those who govern must perform this balancing act, no matter how difficult to achieve; indeed, it is a commitment which is inherent in every oath of office.

Regarding civil liberties concerns, it is clear that no likely future uniform work verification system would require personal data that is not already available in other government data banks. Thus, such a system would either utilize a pre-existing data bank or a new one with less information.

In most cases, opposition to the use of the SSN appears to arise from a fear that, if several organizations possess an individual's number, the ability with which these organizations can exchange information about the individual will be greatly facilitated. Some are concerned that if the SSN is used to expedite unconstrained exchanges of information about people, dossiers about individuals -- in some cases including less than flattering information -- may be created that will follow them throughout life.

Of course, any secure uniform work verification system would be bound by the provisons of Section 3 of the Privacy Act of 1974 (P.L. 93-579). Section 3, codified at 5 U.S.C. 552a (1974), addresses the concerns raised by opponents of a secure uniform work verification system. The statute is very explicit regarding the conditions under which a record may be disclosed, the kind and extent of information an agency may maintain in its records, and the ability of an individual to gain access to his record. Section 3 provides that a governmental agency cannot disclose any record which is contained in a system of records to any person or entity outside the agency without the written consent of the individual to whom the record pertains. It further provides that an agency is to maintain in its records only such information about an individual as is relevant and necessary to accomplish a statutorily required purpose of the agency. And, Section 3 guarantees that any individual can gain access to his record or to any information pertaining to him which is contained in the system.

Additionally, IRCA itself contains specific safeguards intended to minimize the risk of undue invasion of privacy and the risk of government abuse in connection with a secure uniform work verification system: (1) Personal information utilized by the system would not lawfully be available to government agencies, employers, and other persons except to the extent necessary for the purpose of verifying work eligibility. (2) A withholding of verification would not be lawful, except on the basis that the employee or prospective employee had failed to show that he was a United States citizen, an alien lawfully admitted for permanent residence, or an alien authorized to be so employed by the immigration law or the attorney general. (3) The system would not lawfully be available for law enforcement, except to enforce the immigration laws or several statutory provisions relating to false or fraudulent statements or documents. (4) If the system required individuals to present a card or other document, then such document could not lawfully be required to be presented for any purpose other than verification of employment eligibility or the enforcement of several statutory provisions relating to false or fraudulent statements or documents, and could not lawfully be required to be carried on the person.

In any event, a secure uniform work verification system would bear no resemblance to one which utilizes a national identification card with all of its alleged Orwellian implications. Some of those who insist on linking the two concepts perhaps do so for the purpose of chilling the debate on the subject. Almost without exception, these naysayers are the very same ones who opposed the employer sanctions provisons of IRCA to begin with, and who continue to seek repeal today. They have a method to their madness, of course: Although there is clear evidence that employer sanctions are working, they will never realize the true level of their effectiveness without the support of a uniform, fraud-proof work verification system.

4. FAIR's Recommendations

The means to effectively enforce employer sanctions in a nondiscriminatory fashion, and without undue intrusion into the lives of citizens and legal immigrants, are currently available, practical and cost-effective. Moreover, Congress mandated that the federal agencies charged with enforcement of IRCA aggressively develop and adapt existing technology to carry out their responsibilities under the law.

The following are a series of recommendations that could be implemented over the next three to five years, relying on existing technology, to ensure full nondiscriminatory compliance with IRCA.

To ensure that the law is applied in a nondiscriminatory manner, FAIR recommends that the verification procedure be applied to every job applicant regardless of citizenship status.

* **A secure and universal verification system should be established.** A secure and nondiscriminatory identification system could be established using existing, affordable technology and data already available. Such a system should utilize the SSA NUMIDENT data base in conjunction with the INS Central Index System.

* **Current uses of the SSN make it easily suited for this purpose.** A valid SSN is already required to be employed in the United States and can easily be verified through the use of existing, affordable technology. The data in each Social Security file contains sufficient information to determine whether the individual using the number is the person to whom it was issued and whether that individual is eligible to be employed. Employers could ask job applicants a few random, multiple-choice questions, generated by the system and based on information in the record. This, along with a tracking system for multiple use of numbers, would eliminate most abuses.

* **The necessary technology is already in employers' hands.** Verification requires nothing more than a touch tone telephone or a "point of sale device" already in use for credit card verification by millions of retail stores. The verification process, like the credit card verification, could be accomplished in a matter of seconds at a nominal cost. The INS has already conducted a feasibility study and found it to be workable and cost-effective. In fact, the systems and software developed to implement the Systematic Alien Verification System (SAVE) program, which verifies alien eligibility for federal assistance programs, can easily be adapted to verify work eligibility.

* **Verification would be based on the data already in Social Security files.** No physical documentation of any kind would be required. The verification process would rely on confirmation of data, not inspection of documents by an nonexpert. Therefore, there would be no possibility of document fraud.

* **The verification code would be proof of compliance.** Like the verification code issued to merchants by credit card companies, a verification code issued by the INS would serve as proof of an employer's compliance with the law.

* **A telephone verification system would be cost-effective for the employer.** The use of a telephone call-in or point of sale device verification system would eliminate the need for extensive paper work and costly record-keeping. All that would be needed is the inclusion of the INS verification code on an employee's job application form.

* **Secure issuance of new SSNs is necessary.** Tax laws mandate that every individual over the age of two have an SSN. Thus, all new applications for SSNs by an adult must, necessarily, be made by immigrants New applications by adults should be cross-checked by INS.

- **The states should be required to provide death notification to the Social Security Administration.** Each state should be required to include the SSN of the deceased on death certificates and provide that information to the SSA within 30 days after death. Invalidation of SSNs would prevent further use of that number for fraudulent purposes.

- **A national birth/death registry should be established.**

5. Conclusion

It is clear that four years after their institution, the employer sanctions provisions of IRCA are generally effective and enforceable. It is equally clear that whatever flaws exist in the enforcement of sanctions are due to the failure to adhere to the recommendations contained in the law itself regarding the establishment of a secure, effective uniform work verification system. By carrying out the law's mandates through the use of existing technology, employer sanctions can effectively do what they were intended to do -- protect American jobs for American workers and ensure that every individual who has the legal right to work in the United States can compete for a job without fear of discrimination.

Chairman Jacobs. Thank you, Mr. Stein.

Mr. Stein, in asserting that the Social Security Administration should take on this task, I assume that you agree that it would be an additional task to what they are doing now?

Mr. Stein. It should be. I think that certainly verifying the bona fides of documents or numbers they have already issued should be an important part of their job.

Chairman Jacobs. No, no, I say that I assume that you would regard that as an additional task for them though? It is something that they are not doing now and it would be more work.

Mr. Stein. I regard it as a default or an omission that they don't do it and their bureaucratic lack of desire to not want to verify the bona fides of these numbers is inexcusable.

Chairman Jacobs. The thing I am getting at is that some people think that there are about 6,000 people short over there and it is rather clear from testimony before this committee that they don't have enough people and time to answer their phones. There were, I think, 2,500 phones disconnected a couple of years ago at various Social Security offices around the country when they went to the 1-800 number. And we passed a law last year that said that the access to those local offices had to be restored to the level at the time of the discontinuance. There is a little controversy about whether that means what it says. Somehow or another those 6,000 people I guess would have to be hired just to bring the system up to the capability of the responsibilities it already has by law.

Would you support additional tax or what to hire even more people?

Mr. Stein. I think that is an excellent point. And someone who has studied the Immigration Service and the Consular Bureaus now for over a decade, the Immigration Service is now so badly underfunded that they do not even have the ability to carry out basic black letter law that is delegated to them by Congress.

It is a cost benefit analysis of what we believe the cost of the fraud is, both in fraudulent claims and in immigration enforcement deterioration to decide whether or not it is in the best interest of the country to appropriate those funds. We think that it ought to be done and we think the public support is there.

Chairman Jacobs. The educators will say the same thing but going off to borrow money to borrow trouble in other people's wars maybe is not quite so important as educating this Nation and the priorities ought to be reordered. I don't think they will be.

In earlier testimony the question of terrorism was suggested and yet, as I recall when Mr. McDermott said that he passed back and forth on the Canadian border, he did not have much trouble doing that. I think he asked Senator Simpson, would your proposal change that and Senator Simpson insisted that it would not. That it would only apply to employment and hiring situations.

Then I believe Senator Simpson went on to say that we have a potential terrorism problem and his proposal would be helpful in that regard. I suppose the logical question is, how many terrorists come in and go to work and start digging ditches?

Mr. Stein. I think the real question is whether or not the enforcement priorities of finding some way to get a handle on——

Chairman JACOBS. My question is, does this relate to the control of terrorism in your mind, this specific proposal?

Mr. STEIN. The proposal in our testimony, Mr. Chairman, is designed specifically to aid employers in coming up with an approval code which will allow them to hire someone, and to ascertain whether or not they are lawfully entitled to work in this country.

Chairman JACOBS. So your answer is no on that.

Mr. STEIN. The answer is no. We are looking for a person's legal right to be in this country and to work.

The issue of terrorism deals with the entire panoply of border control issues and that goes to border control——

Chairman JACOBS. I appreciate that, but listen to the question. Does this proposal, in your view, touch on control of terrorism?

Mr. STEIN. I suppose it does incidentally. If it does it is perhaps——

Chairman JACOBS. My recollection is that Senator Simpson did stress that and I just wondered what your——

Mr. STEIN. Respectfully, Mr. Chairman, Senator Simpson has also spent a decade studying the fact that——

Chairman JACOBS. Forget the authority, I am just talking about the actual words. You would disagree though that this would make a significant contribution to the solution of any terrorism problem?

Mr. STEIN. I think it is an important first step because the United States, by virtue of its geographic position does not have to worry about terrorism the way that Germany does.

Chairman JACOBS. I think we know that. I think he was speaking in the context to the degree to which the United States does have to worry about terrorism.

Mr. STEIN. It could be supported on that basis.

Chairman JACOBS. Right, but would you agree that most terrorists probably don't come here and apply for work? They probably have their little suitcases and try to leave as soon as possible.

Mr. STEIN. Mr. Chairman, if I were Saddam Hussein wanting to send terrorists to the United States I would not bother sending them through a port of entry. I would simply send them across the southern border at night without inspection.

Chairman JACOBS. In any case if you were a terrorist you probably wouldn't be affected by this legislation, except as you say, just incidentally. You might have to become a movie projector operator to get into the movie, but you are saying that it would only be incidental?

Mr. STEIN. To the extent that this proposal would move us toward getting a national birth/death registry and getting some integrity to the issuance of Social Security numbers and enabling the Government to ensure that people who are citizens have an easy way of proving it and a way that has integrity, clearly it would. After the war broke out, the INS was once again incapable of finding Iraqis who were in this country as foreign students as they were with Iranians back in 1979.

Our whole document system is built on an utter foundation of sand. TRW may have a wonderful set of credit information about me, may know where I am most days of the week, but all they have is a number and nothing that ultimately ties that number to me.

Chairman **Jacobs**. This proposal, as I understand it, the whole documentation in this proposal is based on a valid birth certificate?

Mr. **Stein**. Right, but that is the first step.

Chairman **Jacobs**. Well, maybe we ought to be passing a national birth certificate law.

Mr. **Stein**. As Mr. Gibbons pointed out earlier, a national death registry——

Chairman **Jacobs**. Well, it is too late then. I am talking about for purposes of documentation.

Mr. **Stein**. Not for him. I think it is certainly an important step to link these together.

Chairman **Jacobs**. Let me get some comments from the rest of the panel. What about that? If you don't build a good foundation no matter how glorious your castle is, it falls and garbage in and garbage out. If at the beginning, the birth certificate, itself, is falsified as I believe can easily be done, then what follows is that what follows will be invalid. Does that make sense?

Ms. **Munoz**. Yes, if I may, Mr. Chairman. I think that is right. I think that if we were to implement a secure Social Security card tomorrow what it means is that both the process of document fraud—to the extent that it is occurring—and the process of discrimination just get transferred some place else. They would get transferred to the process of obtaining or replacing the alternative documents. This is one of the reasons that we have been arguing for years that employer sanctions can't work as a form of immigration control because you can't make the system that secure. This is one principal reason, but there are several others which undermine the policy and make these kinds of proposals much more harmful than they are useful.

Chairman **Jacobs**. But is it typical, I don't know. In my State it is typical of a birth certificate to have a foot and hand print, but if there is no verification of that—I mean most birth certificates as we know them in use for obtaining passports and so on are plastic laminated cards issued by the health authorities wherever you came from in your home town.

So what I am wondering is even if this proposal were enacted by the Congress would it not be subject to some of the infirmities that have been described by witnesses so far? In other words, if it is not reliable, could not do a whole lot of good and, yet, obviously could do some harm. Now, if it could do an enormous amount of good and occasionally—the automobile I suppose does some good but runs over people some times too and that is not good—but then there might be a better case for it. So what about the garbage in and garbage out? That is not addressed by this proposal, as I understand it.

Ms. Goldman.

Ms. **Goldman**. One of the proposals that the ACLU has supported for a long time gets exactly to this point. You need to strengthen existing documents. There are a number of identification documents out there that people use all the time, whether it is a driver's license, or a birth certificate, or a passport, or the Social Security number, or the card, and if there are problems with those existing documents that lead employers to think that maybe they are fraudulent or to lack confidence in those documents, let's improve the existing documents at the point at which they are issued, at the driver's license bureau or at the Social Security Administration.

We heard the Commissioner testify this morning that they are trying to improve the quality of those documents. They recognize the problems with them and maybe in another 20 or 30 or 40 years the newly issued cards will be much more accurate. If we improve existing documents, we then allow people to continue to choose to use different forms of identification. We get away from the centralization and away from the national ID issue that is so terrifying to people and which we think will extract much too high a cost in terms of our society.

Chairman JACOBS. Even the driver's licenses with pictures on them only tell you what the person who came and got the driver's license looks like. But Body Heat, does anybody remember that film where the woman had posed with improper identity or had assumed someone else's identity and almost got away with murdering all kinds of people.

Mr. Simcox has not had much of a chance.

Mr. SIMCOX. Your concept of garbage in and garbage out, then suggests that you would conclude that the Social Security Administration now is issuing cards to people in a great many cases where they are based on fraudulent documents?

Chairman JACOBS. I don't even know that it requires a document so much to get a Social Security card traditionally. You just go in and tell them who you are and you get a Social Security number.

Mr. SIMCOX. I have a foreign-born daughter who went through the process of getting a Social Security card and because they tightened the restrictions in 1972, she was required to present a great number of documents, her foreign birth certificate, as well as documents establishing that she is now a citizen of the United States. I was impressed by that. I think it is a good rule, even though it entailed some inconvenience for her and it's the only way that a system like that could really operate.

Chairman JACOBS. I agree but again, the beginning of the whole thing is whether the birth certificate, itself, is authentic. And that was my only question. Are we putting a whole lot of carts before a very fundamental horse, in this proposal?

Mr. STEIN. Mr. Chairman, this committee, I assume it was this committee, authorized the issuance of a Social Security card and I have to get one for my daughter this week for her first tax return at the age of 3. Now, if we are trying to solve this problem over time——

Chairman JACOBS. I think it was age 2, according to my recollection.

Mr. STEIN. Well,——

Chairman JACOBS. You mean you did not get one last year? [Laughter.]

Mr. STEIN. My wife told me I should not come today.

Chairman JACOBS. I won't tell anybody.

Mr. STEIN. For most all native-born Americans the time between the issuance of the number and the birth is declining. So that if you are trying to solve this problem over a period of years, you have got to look both at the birth/death records, the issuance of the Social Security card and the basis on which we issue a driver's license, because we are trying to use them for various purposes, ought to be brought into the overall policy process.

It is really a three-step process and we have got to start sometime, so that we may as well start now.

Chairman **Jacobs**. But there is one step in this proposal, however, is there not?

Mr. **Stein**. Well, FAIR is recommending this as an initial proposal. Now, Senator Simpson's langauge which was objected to at the end of the last Congress would have had a pilot program for the use of driver's licenses being issued with verified Social Security numbers and biometric identifiers. Then we would begin to link the Social Security number and an individual at some point in the process.

Chairman **Jacobs**. You are going to have the last word.

Ms. **Goldman**. Mr. Chairman, you had mentioned to the earlier panel the new rule under the Tax Reform Act of having to get Social Security numbers for new-borns. It might be useful, in this context, to know that the reason that Congress passed that provision was out of concern that parents who were no longer living together were both claiming children as dependents. For that problem, however big it is in the whole scope of problems that the IRS has, that is why children have to have Social Security numbers when they are claimed as dependents now.

We are starting to see that there are reasons, very good reasons, for creating these mandatory identification procedures, but then they lead to things that either were not intended and were not foreseen and then get out of control.

Chairman **Jacobs**. Well, you have made a very useful contribution and we have had a very good hearing today and the committee, I am sure they are all grateful.

[Whereupon, at 1:12 p.m., the hearing was adjourned.]

[Submissions for the record follow:]

STATEMENT OF JON BLAZER, POLICY ASSISTANT CENTER FOR IMMIGRANTS RIGHTS

INTRODUCTION

The Center for Immigrants Rights (CIR) is a New York City-based community organization committed to furthering the rights of immigrants and refugees. CIR was involved in the debate surrounding the enactment of the Immigration Reform and Control Act of 1986 (IRCA), and has been active in monitoring and documenting the discrimination fostered against immigrants and U.S. citizens by IRCA's employer sanctions provisions. Since 1988, CIR has operated an "Employer Sanctions Hotline" in order to provide information about IRCA to workers and employers, and to systematically document IRCA-related discrimination and abuse. Using data collected through the hotline, CIR submitted two reports (in 1988 and 1989) to the General Accounting Office (GAO).[1] This documentation assisted the GAO's preparation of its second and third reports to Congress on the implementation of IRCA.

The question of issuing some form of a national identification card for the purpose of immigration control has surrounded the employer sanctions issue since the early '80's, when proponents of a national identifier argued that such a system would strengthen sanctions enforcement by making it harder for individuals to use fraudulent documents in obtaining a job. Congress ultimately rejected a national I.D. on the grounds that the costs and risks involved were too great to outweigh the possible benefits.[2] Although Congress thus took great care to specify that nothing in IRCA "shall be construed to authorize, directly or indirectly, the issuance or use of national identification cards or the establishment of a national identification card"[3], the deficiencies of employer sanctions have prompted a reactivation of calls for a national identifier. Most recently, some have endorsed an I.D. system as a solution for mitigating the widespread discrimination against citizens and other authorized workers which has so clearly resulted from sanctions.

---

[1] The Center for Immigrants Rights, "The Impact of Employer Sanctions on Citizen and Immigrant Workers: A Report to the General Accounting Office", (September, 1988); The Center for Immigrants Rights, "Employer Sanctions: An Update on its Impact upon Authorized and Unauthorized Workers in the New York Metropolitan Area", (August, 1989).

[2] Report of the Committee on Immigration and Nationality Law of the Association of the Bar of the City of New York, "Methodology, Legal Definitions and Interpretations in Documenting the Employer Sanctions and Anti-Discrimination Provisions of IRCA", (August, 1989).

[3] IRCA, 274A(c).

A system of national identification--whether it be implemented through a "tamper-proof" social security card, a standardized drivers license, or a work authorization card--must be rejected. Such a system would beget more and graver discrimination than it would diminish. It would be unreliable, technologically infeasible, and prohibitively costly, while inviting great intrusions of individual privacy and civil liberties. Furthermore, it would invite enormous public disapproval and protest. We believe these considerations compel Congress to resist the temptation of resorting to national identification as a "quick fix" to complex problems.

In this statement we focus upon the issue with which we are most familiar and which, taken alone, provides compelling reasons to reject any form of national I.D.: discrimination. It is our view that a national I.D. would not substantially remedy the discriminatory employment practices caused by employer sanctions. More critically, it would trigger new and more menacing forms of discrimination, thus placing further hardship upon the very populations it would purportedly protect.

DISCRIMINATION WOULD NOT BE SUBSTANTIALLY REDUCED

Those who envision a system of national identification as a way to redress IRCA-related discrimination argue that employers are wary of document fraud and confused by the large array of documents which currently establish authorization to work; simplification and better guarantees of document authenticity, it is argued, would do away with the tendency of employers to deny work to those who appear foreign. However, while document uniformity may modestly affect that discrimination which stems specifically from employers rejecting bona fide documents[4], it would do little to diminish other pernicious and widespread discriminatory practices which have resulted from IRCA.

The clearest type of sanctions-related discrimination which would remain unaddressed by a national identifier is the selective nature by which employers request any documentation whatsoever from employees. In areas of high immigrant concentration, such as Los Angeles, 16% of employers surveyed by the GAO said they applied IRCA's verification system exclusively to persons whose accent, appearance, or name suggest that they may be foreign.5 Thus, a discriminatory burden has been placed upon those who diverge from what is conceived to be the mainstream norm. Providing a uniform document to all won't have any effect whatsoever upon this burden: some will be asked to produce the I.D., others won't.

---

[4] Even the reduction of this sort of discrimination is premised upon the feasibility of creating a card sufficiently tamper-proof to allay employer suspicion of fraud. As the American Civil Liberties Union (ACLU) observes, numerous studies, most notably those of the Comptroller General, document the technological difficulty, if not impossibility, of implementing a tamper-proof I.D. Further undermining the feasibility of such a task is the estimated billions of dollars required to even attempt the endeavor.: W. Henderson, L. Guttentag, J. Goldman (for the ACLU), "Statement on Voluntary Work Authorization Cards", (November 9, 1989).

In addition, hiring audits persuasively show that employers are screening out applicants who look or sound foreign far prior to the point at which documents even come into the picture. Three separate studies show the extent of differential treatment to be disturbingly high, with accented Hispanics commonly denied the opportunity to even fill out an application for jobs which are available to Anglo job seekers of similar qualification.6 In one GAO example a pair of testers responded to a job advertisement listed under "shipping" requiring a "dependable, hardworking person" and directing applicants to call "Bill":

> The Hispanic tester called the specified phone number and, after inquiring about the job, was told by Bill that the position was filled. The Anglo tester called 15 minutes later and Bill invited him for an interview for later that day. After a 15-minute interview, the Anglo tester was offered the position. The two testers phoned about the job in the same manner to the same person. The only discernable difference in the phone contact was the Hispanic tester's accent (GAO, 1990).

As the example illustrates, sanctions has fostered discrimination which takes place at a stage in the application process earlier

---

5 GAO, 1990. See also: California Fair Employment and Housing Commission, "Report and Recommendations of the California Fair Employment and Housing Commission on the Impact and Effectiveness of Employer Sanctions and Anti-Discrimination Provisions of the Immigration Reform and Control Act of 1986", (1990).

6 U.S. General Accounting Office, "Immigration Reform: Employer Sanctions and the Question of Discrimination", (March 1990); the City of New York Commission on Human Rights, "Tarnishing the Golden Door: A Report on the Widespread Discrimination against Immigrants and Persons Perceived as Immigrants which has Resulted from the Immigration Act of 1986", (August, 1989); A. Kamsvaag (CHIRLA) and A. Mischel (LAFLA), "Employment Discrimination Against Immigrants: A Study of the Job-Seeking Experience of People who Speak English with an Accent", Preliminary Report, (March 15, 1990).

than that which could be meaningfully affected by more reliable documentation.

Furthermore, an important employer response to sanctions has been to adopt "citizens only" hiring policies. In fact, last year the GAO reported that 14% of employers surveyed began to hire only U.S. citizens and not to hire persons with temporary work eligibility documents as a result of IRCA, a practice particularly injurious to Asians, Hispanics and other minorities (GAO, 1990). This illegal policy is caused in significant part by the misconception that IRCA requires employers to only hire U.S. citizens. Clearly, for employers who have adopted "citizen-only" hiring policies for this reason, it matters little what type of documentation non-citizens have.

Finally, and perhaps most importantly, a system of national identification fails to address and confront the more insidious discrimination spurred on by employer sanctions. In our last report to GAO, we emphasized the important role played by personal bias in enhancing the discriminatory implementation of sanctions:

> Pre-existing racial biases and prejudices about who is perceived as an immigrant versus citizen, "foreign" versus native, and illegal versus legal, combine with employer ignorance about documents so that racial minorities and/or those who "look foreign" or "sound foreign" are deemed more suspect; they disproportionately bear the burden of unfair or illegal employment practices arising from employer sanctions (CIR, 1989).

Employer sanctions have promoted the notion that the hiring of non-natives is an undesirable, indeed risky business which makes employers liable to penalties. In doing so, it has reinforced already existing prejudices and therefore provided a "legitimate" reason for discriminating to employers who are already inclined to do so. A national I.D. would further reinforce bias, regardless of whether one's documents are perhaps more comprehensible and reliable.

NEW FORMS OF DISCRIMINATION WOULD OCCUR

The creation of a national I.D. would bring new and graver forms of discrimination upon the racial and ethnic minorities already burdened by the atmosphere of prejudice IRCA has nourished.

First, much of the discrimination prevalent in the hiring procedure would simply be transferred to the procedure of obtaining a national I.D. card. A "tamper-proof" card will only be as accurate as the underlying documents upon which it is based. Since these documents, such as the birth certificate, can themselves be forged, it is likely that those of "foreign" looking persons would be suspect to excessive scrutiny:

> Persons who appear 'likely to be undocumented' by virtue of their appearance or speech accent may be required to present more supporting documents than their Anglo counterparts, and could be subject to delays in receiving the card while their documents are being checked.7

Those who present primary documents from other countries are also likely to face differential treatment, as the agency administering the documentation will not be as familiar with discerning the authenticity of the certificates.

When newly authorized workers, i.e. political asylees and permanent residents, attempt to get employment eligibility documents, they already face the formidable obstacles of INS information mismanagement, deficient data verification, and processing backlogs. Under a system of national identification, these individuals, often in urgent need of work, would have to apply for an I.D. through a system that would be, in all likelihood, more centralized, more overburdened, and further delayed. This hardly seems to be an intelligent remedy for a situation in which, according to the New York State Inter-Agency Task Force on Immigration Affairs, many authorized workers are being denied jobs solely because of their inability to obtain immigration documents fast enough.8

For temporary workers, such the Salvadoreans, Liberians, Kuwaitis, and Lebanese recently granted temporary protected status, the procedure for getting and maintaining proof of work authorization would be even more arduous. As the GAO observes, "there are millions of aliens who have temporary work eligibility status who would have to be issued Social Security cards with an expiration date and then reissued new cards if their temporary status is renewed" (GAO, 1990). Thus, an increased hardship is placed upon the very individuals already most economically vulnerable to discrimination caused by IRCA.

---

7 The Institute for Public Representation, Memorandum to the National Council of La Raza, Georgetown University Law School, November 7, 1989, paraphrased in: C. Munoz (for the National Counsel of La Raza), "Testimony on the Use of the Social Security Number as a National Identifier", (February 27, 1991).

8 New York State Inter-Agency Task Force on Immigration Affairs, "Workplace Discrimination Under the Immigration Reform and Control Act of 1986: A Study of its Impact on Workers", (November, 1988).

One of the greatest sources of opposition among Americans to a system of national identification comes from the suspicion that a national identifier would eventually be used for purposes other than mere employment verification.[9] In its testimony to this Subcommittee, the ACLU rightly warned of the ease with which a national I.D. could be transformed into a de facto domestic passport.[10] Allegedly tamper-proof, law enforcement officials would likely view the I.D. as a preferred or even required proof of identity and legal status. Again, the burden of such a practice would fall disproportionately upon Asians, Hispanics and others suspected to be "foreign". Individuals from those racial and ethnic backgrounds, particularly those living near border areas, would feel required to always carry their I.D. as a form of self-protection against "spot-checks". Moreover, there would be little legal recourse against increased harassment, interrogation, and searches (already on the rise at the borders), for "current law allows police to stop individuals without any particular suspicion that a crime has been committed, and to request identification, as well as to detain and search people who fail to produce proper documents" (ACLU, 1989). A national I.D. would greatly encourage the questioning, searching, and detention of persons deemed "suspicious"-- a policy which many minorities know from experience to be discriminatory.[11]

CONCLUSION

It is our conviction that the only effective response to the discriminatory hardship caused by employer sanctions is to repeal the law, and we are hopeful that Congress will in due course concur. However, it appears for the time being that Congress is likely to continue its search for other remedies to IRCA-related discrimination, such as the Immigration Act of 1991's expansion of anti-discrimination protections, and its provision of funds for education outreach efforts concerning these protections. While these measures are likely to prove insufficient, we welcome them in the interim and urge Congress to allocate funding for this education in a timely and complete matter. We further urge this Subcommittee in particular to resist the temptation of adopting attractive "solutions", such as a national identifier, which will only serve to worsen the very problems they are intended to ease.

---

[9] Although there are in fact some proponents who explicitly propose that improved work authorization data be put to the service of broader public administration and law enforcement purposes. See, for example D. Simcox, "Secure Identification: A National Need-- A Must for Immigration Control", Center for Immigration Studies, (October, 1989).

[10] J. Goldman (for the ACLU), draft of Testimony on the Use of the Social Security Number as a National Identifier, (February, 1991).

[11] As Cecilia Munoz of the National Council of La Raza recently testified before this Subcommittee, many Hispanic Americans "have experienced routine misuse of identification cards in border areas, where U.S. citizen Hispanics were once encouraged to carry cards to prevent being mistakenly classified as undocumented immigrants and subsequently detained and deported": NCLR "Testimony on the Use of the Social Security Number as a National Identifier" (February, 1991).

Congress of the United States
Congressional Hispanic Caucus
House Annex II — Room 557 Washington, D.C. 20515 (202) 226-3430 FAX: (202) 225-7569

STATEMENT OF

SOLOMON P. ORTIZ

BEFORE THE SUBCOMMITTEE ON SOCIAL SECURITY
COMMITTEE ON WAYS AND MEANS

FEBRUARY 27, 1991

Mr. Chairman:

Thank you for inviting me to present testimony here today as Chairman of the Congressional Hispanic Caucus .

The issue being discussed here today, the need to establish a national ID card and whether that card should be a person's social security system number, is of primary importance to the Members of the Hispanic Caucus.

There are two basic concerns involved with this proposal. The first has to do with expanding the use of the social security system. This would require the establishment of a massive and reliable federal data base to deal with the bureaucratic nightmare which would result from expansion of the current system.

This system would have to be linked to the States and Puerto Rico and would require instant access to verify and share information. The cost involved in such an undertaking would be extraordinary. Assuming that funds are available, the inherent problem of fraud would remain. The underlying documents required to obtain a social security number can still be forged or may contain errors. Moreover, a method of verifying existing numbers would have to be devised. This in itself would be a difficult task. It has been estimated that as much as 75% of social security numbers have been issued before evidence of age, identity and citizenship or alien status was required.

The second concern and one of primary importance is the probable encroachment in the area of civil liberties. A national ID program has been suggested as a viable method for dealing with the problem of illegal immigration. Everyone would have to have a number which would serve as a verification for work authorization. This assumes that employers would abide by the work authorization requirement in their hiring practices. We all know this is not the case.

The very notion of a national ID card raises images of countries such as South Africa where they have abolished such practices. Proponents state that because it is national in scope and that everyone will be required to have one, that this will not result in discrimination. But I say to you, that what is being advocated by this program is a blue print for discrimination.

Initially everyone will have to submit to some sort of electronic fingerprinting. We are not talking about actual fingerprints, for that is old technology and obsolete. We are talking about biometric fingerprinting, such as retina screens, skull measurements, etc. Once that process is completed, this ID card will be required for all sorts of reasons, drivers licenses, medical purposes, credit information and work authorizations. Each of this uses increases the potential for discrimination violations.

We are all familiar with the GAO's findings regarding discriminatory hiring practices against foreign looking and sounding persons. While the GAO report dealt with the employer sanction provisions, this proposal would escalate the problem to national proportions.

There are too many negatives built into this proposal and no visible positive effects. I am convinced that a national ID card is something which most Americans will not stand for. The infringement upon the civil liberties of individuals should be the overriding concern here and therefore, we should not adopt a national identification program..

Thank you for allowing me this time.

NATIONAL IDENTIFICATION CARDS

by

Larry F. Linden

The following comments relate to the proposal to create a national identification card and subsequent collateral issues. A national I.D. card suggests identification policies from birth to death. Such cards would efficiently provide individuals secure access to entitlements and reduce fraud associated with the use of false identification.

NATIONAL I.D. CARD - THE ARGUMENTS

The real issue here is not whether there will be a State or National identification document. Such a debate can dissipate considerable resources. A *phased* state/federal individual identification plan can enhance the many benefits of living in the computer/information age. Legislative effort should be directed to *national standards* for positive electronic identification of individuals that will assure secure access to state/federal government entitlements - Electronic Benefit Transfer Systems. Such a phased program would require several years for proper implementation.

In the United States, one's birth is recorded in the state of such birth. This is the point at which appropriate identification does commence, however the assignment of an official government number to the individual does not occur until work or driving eligibility is requested.

The so called "card" cannot be designed and implemented in a vacuum. The card is only a secure key to government benefit systems. Eligibility for such benefits resides with each government agency i.e. USDA Food & Nutrition Service (Food Stamps) Driving privileges, Retirement benefits, Medical services etc. The focus of this effort must be on interactive systems. This begins with the construction of an appropriate numbering system that prevents individuals from fraudulently obtaining government benefits through the use of false identification and/or multiple enrollment in more than one state of residence.

The following comments are targeted to create a national identification system that harnesses the collective state/federal computing power to the benefit of individuals and government alike.

IDENTIFICATION TECHNOLOGY

The ability of current or future technology to identify individuals is a given. Technology is here to provide any level of identification we think appropriate. Finger, Voice, Hand, Eye, Signature and special pattern techniques are commonly called "biometrics".

While biometrics can and will play a part in the identification of an individual the real issue is reliable and secure *access* to key databases. The act of absolute identification should be invoked only when there is sufficient doubt. If systems were operated with a requirement of positive identification for every access, they would be so burdened that little would be accomplished.

Identification can be greatly aided by new technology - particularly Electronic Imaging and Automated Fingerprint Identification Systems. It is quite practical for an electronic image and print file to reside in each state. Such a file would not be used for ordinary transactional access such as food stamps or social security payments. It would be for the purpose of positive identification of any individual when qualifying for such services.

A computer oriented number must be assigned at birth. Electronic image/print files can be implemented at the point of first significant government benefit request. These files should be updated at least every ten years.

Birth Recordings, Work enrollment (Social Security), Driving Privileges and government benefits must be reviewed with the intent of having one common numbering system that can be used for a multiplicity of government services. This does not mean a single number for all categories. It does mean the same numbering format for all individuals combined with a prefix or suffix that denotes the service or benefit in question. The image/print file would be available in one location only -state of residence. Procedures and protocols can be effected to transfer such files when a person relocates to another state. Such procedures would also permit government to government access for special identification purposes.

The future Motor Vehicle Administration may well be the collection point of such image/print data. In fact MVAs may, at some point in time, be known as "Records and Identification". Such an entity could serve as an effective benefit service bureau that administers many benefit programs when eligibility is so certified. Costly duplication of such services would be eliminated.

The technology is available. Legislation and standardized identification practices will bring about the profitable use of computer power. Individuals and government alike will benefit.

SOCIAL SECURITY'S ROLE

The role of the Social Security Administration should not be substantially changed. After all, SSA is the ultimate database that will provide benefits for all citizens based on their retirement, disability, and medical eligibilities.

SSA, as any other state or federal agency, would electronically communicate with various other agencies, both federal and state, in order to certify eligibility and prevent duplicate payments. A common numbering system combined with a shared State Records & Information Database would assure efficient and secure information and identification data access on a need to know basis.

PRIVATE COMPANIES ACCESS TO GOVERNMENT IDENTIFICATION NUMBERS AND DATA.

Legislation would be necessary to prevent SSA from providing the private sector with data about any individual except the necessary interaction for "employer/employee administration".

The proposed "National Individual Numbering Standard (NINS) would be strictly for government use - not to be commercialized. This standard would protect the privacy of individuals, while at the same time giving them ready access to entitlements when appropriately qualified. Private companies should not be allowed the use of the NINS number. Image/print databases would not be commercialized in any way.

SUMMARY

A national identification system has long been misunderstood.

Some people feel that a nationally issued high tech card would solve all problems. This is far from the truth. 250,000,000 data bases (smart memory cards) is impractical and invites unlawful multiple enrollment, excessive cost and unreliability.

The law would require all persons to immediately report a change of address. Such changes would be subsequently electronically communicated by R & I to other appropriate agencies. R & I computer files would reflect current and past residents. At some point in time, past resident files could be archived.

A review of all current privacy legislation would be necessary to construct a plan that would phase in a foregoing "state operated/federal standard" individual numbering system. The review would seek to avoid conflicts, assure rights and privacy, certify data integrity, provide ample time for local agencies to convert to new system, and most importantly to be certain that most individual/government needs can be accomdated for many years to come.

When the identification system is clearly defined, a simple but reliable and secure card for access can then be employed. One should not mislead by the commercial on/off line arguments. The United States is indeed a wired society. We are computer dependent. Maintaining large distributed secure identification databases with proper redundancy and networking is a well known concept. Data processing management is experienced.

There is a widespread "big brother" syndrome. A distrust of information collection at the federal level. Privacy should be so protected by the *private* sector.

The focus must be on how to best utilize computer power, both state and federal, to provide positive individual identification, secure access to government benefits, low cost administration of benefit programs, protection of individual privacy, effective fraud detection, and of much importance - a system that truly performs as a fraud deterrent.

National identification is important to all parties concerned. The benefits in terms of cost savings and access efficiencies are distributed to individuals, state and federal administrations. Participation of all parties in the development process is vital. A national identification numbering standard and a network of image/print databases will produce a new era of secure and efficient government benefit delivery.

STATEMENT ON THE USE OF THE SOCIAL SECURITY NUMBER AS A NATIONAL IDENTIFIER

Presented to the
Subcommittee on Social Security
U.S. House of Representatives

Presented by
Mark H. Epstein, Sc.D.
Executive Director
National Association of Health Data Organizations

March 13, 1991

On behalf of the National Association of Health Data Organizations (NAHDO), I appreciate the opportunity to comment on the use of the social security number as a national identifier. My remarks are restricted to the use of the social security number as a tool to improve health care.

I. BACKGROUND: STATE HEALTH DATA ORGANIZATIONS AND NAHDO

NAHDO owes its existence to the growth of public access health care data, and exists to enhance the growth and development of health data organizations. It is only since the early 1980s that more than a handful of states have had public domain health care data at their disposal. Most of the early systems included hospital financial and statistical data but seldom included hospital discharge data. During the 1980s that small handful has increased to include more than 30 states with health care databases. [States with public access hospital discharge data bases include Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Maine, Maryland, Massachusetts, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, and Wisconsin. Most of these states also collect hospital financial data. Minnesota and Virginia only collect hospital financial data at this time. Other states, such as Alabama, Kansas and Nebraska, are considering the development of hospital discharge data systems.]

The proliferation of statewide data bases and other large data bases has presented new opportunities to understand better use, costs and case-mix of hospital care, and to assess which data are useful as indicators of quality of care. NAHDO emerged in response to needs identified by the professional staff responsible for implementing these new public data organizations who sought to learn more about current techniques and the most effective and efficient ways to achieve their objectives. The Washington Business Group on Health and the Intergovernmental Health Policy Project at the George Washington University established NAHDO in 1986. In 1988, NAHDO became a distinct private, nonprofit educational and charitable membership organization, which is governed by a nine-member Board of Directors.

NAHDO is dedicated to improving health care through the collection, routine dissemination, public availability, and use of health data The Association provides leadership in health care information management and analysis, promotes the availability and accessibility to health care data, and the use of these data to make informed decisions, practice prudent purchasing and guide health policy development. NAHDO pursues its mission by:

- o Supporting the development of public health data organizations and use of their data bases to address national, state and community issues, and individual concerns;
- o Promoting uniformity and standardization of health care data collection and dissemination among public, private and voluntary data collectors and users; and
- o Providing timely access to the latest developments, trends and expertise in health information.

NAHDO's members include Federal and State health data organizations, health services researchers, third-party payers, state hospital associations and hospitals, business coalitions, employers, trade groups, professional membership organizations, software vendors, consultants, and health information/cost management firms.

II. THE SOCIAL SECURITY NUMBER AS A UNIQUE PATIENT IDENTIFICATION NUMBER

A. Rationale for Using the Social Security Number as a Unique Patient Identification Number

State health data organizations collect detailed patient data from hospitals and other service providers. These data are valuable resource and may be used in a multiplicity of ways by public policy makers, purchasers of health care services, local and statewide health councils, business and health care coalitions, professional and trade associations, health services researchers, third-party payers, and health care providers.

The social security number is a critical data element in a patient data base. Maximum use and completeness of the data are contingent on a unique patient identifier which promotes the capability to link distinct records for a patient. Such linkage is a prerequisite to construction of a data base built on episodes of care or illness. The goal of this data base is to provide a complete picture of an individual's health care. The social security number is the tool which permits an individual's medical experience across different institutions, providers and payers to be aggregated into a single comprehensive record.

Lacking a unique patient identifier, the use of a data base for health services research and planning is restricted because the data can be misinterpreted easily. For example, chronic conditions with recurring admissions are not identifiable on existing hospital discharge data bases. The patient population with an acute exacerbation of a chronic disease, such as chronic obstructive pulmonary disease (COPD), could appear larger in the aggregate than is actually the case. A competing explanation, which is more likely to be the case in this situation, is that fewer individual cases with COPD are presenting to the hospital but this patient population are admitted at a higher frequency (i.e., readmission for the same condition).

Using the social security number as a unique patient identifier provide s greatly expanded flexibility to track acute care patient readmissions, both within the data base and among facilities, and provides statistically acceptable information on new cases versus readmissions to data users. Having the ability to link data bases would increase the value of existing data bases and provide us with a better understanding of the health care system: how it is succeeding and how it is failing. Key to acquiring a better understanding is information -- information that can be used to identify commonalities and differences in service delivery, costs and patient outcomes. Improving existing data is a prerequisite for moving toward a goal of becoming a healthier nation.

B. NAHDO-Sponsored Research Initiatives

NAHDO supported two research initiatives, the Hartford Panel of Experts and the NAHDO Ambulatory Data Committee, which endorsed the need for a unique patient identification number as a necessary tool to create a comprehensive record of a person's medical care within and across health care systems.

1. Hartford Panel of Experts

NAHDO in conjunction with the Washington Business Group on Health and under the sponsorship of the John A. Hartford Foundation convened a national panel of experts to develop recommendations, which if accepted widely and implemented, would improve uniformity of health data, particularly patient-level data. The panel included representatives of the American Hospital Association, Kaiser Foundation Health Plan, Florida Health Care Cost Containment Board, United Auto Workers, Health Insurance Association of America, Colorado Health Data Group, Blue Cross/Blue Shield Association, Midwest Business Group on Health, Joint Commission on the Accreditation of Healthcare Organizations, Deere and Company, and the National Center for Health Statistics.

In its report, Fostering Uniformity for Health Care Assessment Data Gathering, May 4, 1989, the Panel of Experts emphasized the

> value of being able to capture all records pertaining to an episode of illness, both for acute and chronic conditions. This requires a unique person-identifier on each record, rather than the patient account number, which is most common on UB-82 (HCFA Uniform Bill) and UHDDS (Uniform Hospital Discharge Data Set) data systems.

The Panel considered alternate ways to build complete records of care for an individual and agreed that "a much stronger means to link data is a unique identifier for each person, which is automatically used regardless of where the patient obtains care." The Panel of Experts concluded that:

> Recommendation #5: To effectively monitor and evaluate the totality of care an individual receives from different providers or delivery systems, the Panel recommends that a strategy be developed for a unique Personal Identification Number (PIN) system to be used by providers, insurers, purchasers and regulators...

Comments received from participating organizations, which are part of the report, supported the Panel of Expert's recommendation for the development of a unique patient identification number. Carl Schramm, President of the Health Insurance of America, wrote:

> ... While HIAA does not have a specific policy on the development of a unique personal identification number, recommendation 5 is consistent with HIAA's "Major Elements of a Model Hospital Data Disclosure Bill" which contains a patient identification number among its specifications. Indeed, a number of states such as Washington, California and Pennsylvania are already requiring personal identification numbers to be reported to their state data systems. The advantages of linking patient records over time and through various levels of provider treatment adds significantly to the ability to measure cost, quality and access.

James D. Mortimer, President of the Midwest Business Group on Health, wrote that:

> A PIN would be valuable for data research and for linking episodes of care. This is probably the most important recommendation in this study. The use of magnetically encoded "smart cards" for public/private benefit plan identification which contain the PIN and demographic data ... would improve the completeness and accuracy of this data operationally...

The Panel of Expert's concern about patient confidentiality is summarized in the letter from Regina McPhillips, Dr.P.H., Director of the Bureau of Data Management and Strategy of the Health Care Financing Administration. Dr. McPhillips wrote:

> We are concerned that no mention has been made of privacy or confidentiality restrictions in the recommendation to provide patient level data in an easily retrievable automated format (Recommendation #1). We are concerned that this, combined with the recommendation to develop a unique personal identification number, could be read to imply the opening of patient-specific files to a wide variety of people and may violate the confidentiality of personal information. Privacy and confidentiality restrictions will need to be imposed on all researchers and others using data derived from patient records systems...

It bears emphasizing that both States and Federal agencies are concerned about patient confidentiality and have enacted laws to protect the basic rights to privacy of the individual patient. Access to patient-specific data is not possible. Nonetheless, the development of a unique patient identification number and its use in linking medical records to create episodes of care and the concern for individual privacy are not inconsistent. Procedural and technological applications can be employed to promote record linkages and ensure patient confidentiality.

2. NAHDO Ambulatory Data Committee

Ambulatory health care has experienced significant growth in recent years. (Ambulatory health care is defined as all care provided to patients who are not hospitalized or institutionalized as inpatients in a health care facility, which is the site of the encounter.) The growth is attributable in part to the continuing transfer of services traditionally offered on an inpatient basis to ambulatory settings. The ambulatory care "universe" is extremely large and highly fragmented. The size and consequent economic weight of the sector make it imperative that reliable data for monitoring and improving quality of care, controlling costs, ensuring access and developing useful analytical tools are collected. The fragmentation, however, makes this task extremely difficult.

The NAHDO Ambulatory Data Committee was created in March 1987 to assist state data agencies in the collection, analysis and dissemination of ambulatory care data. The Committee addressed administrative and clinical data issues, and developed positions in response to the interests of State, Federal and other public and private organizations which gather health data.

The Committee members included representation from the Wisconsin Center for Health Statistics, Health Care Financing Administration, Florida Health Care Cost Containment Board, American Medical Record Association, National Center for Health Statistics, Health Insurance Association of America, Corporate Cost Management, Colorado Health Data Commission, New Hampshire Office of Health Services Planning and Review, Massachusetts Rate Setting Commission and West Virginia Health Care Cost Review Authority.

In October 1989, NAHDO released the report of its Ambulatory Data Committee, Developing A Uniform Approach for Collecting Ambulatory Health Care Data. The Committee heard testimony on an array of topics associated with the standardization of data bases, classification of ambulatory care services, allocation of available resources and activities (initiatives) of state health data agencies. Among its findings and conclusions, the Committee emphasized the need for a uniform core data set, the use of uniform data base structure and coding, the need for a consistent point of collection (i.e., point of service), and the need for a unique patient identification number. [NOTE: The Committee defined a unique patient identification number as a "unique number for the individual that links personal characteristics of the person to all services received by the person within a health care system and across systems.]

Specifically, the Committee stated in its report that:

> There is a growing understanding that a reliable, uniform, and unique patient identification number will assist greatly the documentation of ambulatory health care. With a unique patient identifier, the potential exists to link records of different practitioners, analyze services provided to an individual over many encounters to create an episode of care, and analyze services to a population at a point in time or over time.
>
> Yet patient identifiers have well-recognized shortcomings. The identifier most often proposed, the Social Security number, could give the social welfare system access to the patient's medical record, breaching confidentiality and compromising the right of privacy. Identifiers based on new numbering systems face major logistical and financial objections.
>
> In spite of these problems, the NAHDO Ambulatory Data Committee supports the use of Social Security numbers provided stringent measures to protect individual identity are adopted. These privacy protections should be established within State and Federal law.

C. Patient Confidentiality

Ensuring patient confidentiality is recognized in State and Federal laws. Patient specific records collected by state health data agencies which contain identifying information are exempt from public disclosure by state law. Can patient-level data be linked across providers and patient confidentiality ensured by a state data agency. The answer is unequivocally yes.

For example, the State of California Office of Statewide Health Planning and Development is responsible for collecting, analyzing and disseminating hospital discharge data. By state law, this agency prohibits public disclosure of social security number, date of admission, date of procedure and data of discharge, data which could be used to identify an individual. The agency seeks to balance the need for access to data and the application of these for appropriate uses with the rights of patients. For purposes of linking data, the agency takes a patient's social security number and encrypts (codes) it into a record linkage number. The creation of a record linkage number makes impossible the identification of any patient. California's technique of encryption may be used by other state data agencies.

III. SUMMARY STATEMENT

NAHDO encourages the use of the Social Security Number for use as a unique national identification number. We have presented information about the need for and value of having a unique patient identification number as a tool to help improve health status. It is reasonable to build on an existing system, the Social Security Number, rather than developing a new system. The concern for patient confidentiality is written clearly into State and Federal laws. Public release of health data must meet rigorous tests. Nonetheless, there are ways to link patient data and preserve patient confidentiality. California's procedure for encryption of the Social Security number into a new record linkage number is an example of how to improve the value and utility of health data while ensuring individual rights are protected.

[THE REPORTS THAT WERE ATTACHED TO THIS STATEMENT ARE BEING RETAINED IN THE COMMITTEE FILES.]

NORTH TEXAS IMMIGRATION COALITION
3845 Oak Lawn Avenue
Dallas, Texas 75219

March 14, 1991

USE OF SOCIAL SECURITY NUMBERS AS IDENTIFIERS

The North Texas Immigration Coalition (NTIC), a broad-based coalition of attorneys, businessmen, educators, and social service providers, has monitored the implementation and consequences of the Immigration Reform and Control Act (IRCA) since 1986. We thank the Subcommittee for the opportunity to comment on this matter.

In 1986, Congress passed legislation aimed at curtailing illegal immigration by outlawing the market for undocumented labor, which was then thought to be the engine driving the influx of undocumented foreign workers. It needs hardly be restated that the four years since IRCA's implementation have seen illegal immigration continue apace. Moreover, IRCA's employer sanctions provisions have fostered a previously unknown type of discrimination: the refusal to hire the foreign-born, including naturalized citizens, aliens authorized to work, those who speak with unfamiliar accents, in short, those who "seem foreign".

Repeated GAO studies have found that such discrimination is as insidious as it is widespread. One-seventh of the employers surveyed in 1990 reported that they now hire only U.S. citizens (in violation of the law). Nearly one-tenth of employers surveyed admitted scrutinizing the identity and/or employment documents only of those applicants who appeared "foreign". Puerto Rican U.S. citizens report that prospective employers, unaware that Puerto Rico is a part of the United States, often demand multiple forms of identification.

Some have claimed that a "counterfeit-proof" national identity document (or number) would obviate such discrimination while rendering still more unlikely the possibility that an undocumented worker might enter the labor force. The logic underlying this claim is fundamentally flawed. Furthermore, pursuit of such a utopian scheme would foster the very ill it is purportedly designed to eliminate. Finally, the proposal violates cherished American notions about the citizen's relation to his/her government.

Currently, employers are required to ascertain that job applicants are eligible to accept employment in the U.S. Immigration and Naturalization (INS) Form I-9 (Employment Eligibility Verification) lists over a dozen acceptable

A Member of The National Immigration, Refugee, & Citizenship Forum

documents, including "other". If a single document (or "verifiable" number) were to replace most or all of those listed on Form I-9, would not confusion, mistakes, and discrimination be eliminated at a stroke?

The question begs another: how would such a document (or number) be issued? Social security numbers are currently issued to U.S. citizens upon presentation of state-issued identification documents, birth, citizenship, or naturalization certificates, and to foreign nationals upon presentation of INS documents. If these and other documents are easily counterfeited (as alleged), how then could the Social Security Administration (or other government agency) eliminate this fraud when it has no control over the issuance of underlying documents? Birth certificates would continue to vary widely from county to county and state to state. Would state health departments require multiple identity documents of birth-certificate-requesters? Perhaps such things would be required only of foreign-seeming applicants.

Plainly, the discrimination described above would obtain under the proposed universal system. However, the agent of discrimination would be a distant government bureaucracy rather than a well-meaning employer. Under such conditions, purveyors of forged documents would have greater incentive to perfect their criminal methods. Meanwhile, only the "foreign-seeming" would be required to show the document; certain ethnic groups would remain "above suspicion". The proposed document would be voluntary in theory only.

Following the passage of IRCA, the Systematic Alien Verification for Entitlements (SAVE) program was implemented. In theory, SAVE would prevent ineligible aliens from receiving public benefits. In 1987, the GAO found SAVE to be inaccurate and unreliable. Nearly one-third of verification requests required a secondary check owing to faulty or incomplete information in SAVE's data bank.

The INS' inability to manage its case backlog and data banks was also well documented by the GAO as recently as 1990.

The American people have clearly been demanding for many years that government bureaucracy loosen its stranglehold on the free movement of people, goods, and services. The government agencies most likely to implement the policies contemplated are precisely those agencies characterized by mismanagement and waste. By way of response to these characterizations, proponents of a national identifying number suggest streamlining the bureaucracy, that is, giving the government more intrusive powers to oversee the everyday affairs of ordinary people.

As freedom and democracy expand to countries and continents where they had been unknown, it is astounding that the Congress of the United States would consider imposing a system reminiscent of the former Pass Laws of South Africa. In less hysterical times, Congress recognized the potential for abuse of the employer sanctions provisions of IRCA: the Act mandates that employer sanctions be repealed if they are shown to have caused widespread discrimination. Moreover, IRCA clearly states that nothing in the Act shall be interpreted to endorse or lead to the development of a comprehensive identification system.

The North Texas Immigration Coalition believes that any attempt to limit illegal immigration should focus on the root political and economic causes of that immigration. Attempts to limit illegal immigration by shrinking the civil rights of law-abiding citizens and aliens are destined to fail, for the American people will not accept perpetual surveillance in exchange for the transitory benefit envisioned by the proponents of the policy contemplated.

by: ______________________
Jonathan Bernstein

STATEMENT OF DAPHNE KWOK, EXECUTIVE DIRECTOR ORGANIZATION OF CHINESE AMERICANS, INC.

INTRODUCTION

The Organization of Chinese Americans, Inc. (OCA) is a national, non-profit, non-partisan organization of Chinese Americans. Since our formation in 1973, OCA has been dedicated to promoting the active participation of Chinese Americans in civic affairs at all levels and securing justice, equal treatment and equal opportunities for Chinese Americans and all Asian Americans. OCA has been involved with immigration issues and monitoring discrimination resulting from the Immigration Reform and Control Act of 1986.

At this time, OCA respectfully submits to the Committee on Ways and Means the following statement against the use of the Social Security Number as a national identifier.

STATEMENT

The idea of establishing a national identification card has been a part of the immigration debate since the 1980's. Even with the passage of the Immigration Reform and Control Act of 1986 (IRCA), the debate has continued, fueled in particular by the purportedly unintended, but never the less, discriminatory side effects of the employer sanctions provision of the IRCA Act.

Employer sanctions was established as a means of controlling illegal immigration by making the employers verify the identity of potential employees and their eligibility to work in the United States. Valid documents of proof include passports, birth certificates, driver's licenses, voter registration cards, and social security cards. Employers failing to comply with verification requirements may be liable for sanctions.

A number of studies, including a 1990 report by the U.S. General Accounting Office, have concluded that employer sanctions have caused widespread discrimination against racial and ethnic minorities. Employers seem to be more suspicious about the authenticity of documents provided by prospective minority employees. In order to protect themselves, many employers have engaged in practices resulting in employment discrimination and lost job opportunities for "foreign looking" job seekers, especially Asians and Hispanics, who are American citizens or are legally authorized to work.

Proponents of a national identifier believe that a standard government issued ID card would ease the confusions over the reliability of existing documents, and hence, alleviate the discrimination resulting from this policy.

But a national ID card would not work because: 1) it may reduce discrimination based on employers' fears of fake documents but it would not impact discrimination based on "foreign" appearance, name, or accent, and 2) instead of eliminating document fraud, it would create more: a national ID presupposes the use of other underlying documents to establish identity, i.e. birth certificates, driver's licenses, Social Security Number, etc. But the ideas of a national ID card was posited because of fraud problems with precisely those latter documents to begin with. Fraud would now be associated with both the underlying documents and the national ID card.

But aside from the failure to "fix" immigration problems, the whole idea of a national ID card, especially using the Social Security Number (SSN) as one, is highly disturbing. Serious questions of civil liberty and individual rights violations are immediate and apparent.

Even though the SSN was created for the sole purpose of tracking workers' earnings for the collection of taxes and benefits in the Social Security Program, the number has now, more or less, become a de facto national identifier.

The SSN's expanded use as a numerical identification system by the public and private sectors is well known. All federal agencies use the SSN for identifying individuals. The IRS utilizes the SSN for taxpayer identification. Persons applying for federal aid programs must have a SSN. Many states use the SSN as a driver's license number. Most banks, credit bureaus, hospitals, and educational institutions use the SSN for identification as well. Presently, the SSN basically provides carte blanche access to private and confidential background information on any individual. With the use of increasingly sophisticated computer technology for information processing, the potential for abuse and violations of privacy and civil liberties is quite alarming.

Indeed, precedent already exists where government collected information has been used for purposes other than that which it was originally intended. During World War II, a variety of supposedly confidential governmental and private information was used to round up Japanese Americans for relocation and internment on the basis of race. During the Watergate years, there were illegal disclosures and uses of IRS documents and other government records for political ends. During the Vietnam War, the FBI used its computerized National Crime Information Center to maintain surveillance on anti-war activists. Even the Social Security Administration was guilty of disclosing SSN information to the private sector for commercial use. The specter of George Orwell's "Big Brother" is not all that inappropriate.

Lastly, given the history of racism in this country, racial minorities will be especially vulnerable to discriminatory abuses arising from a national ID card. It is not that difficult to visualize scenarios where law enforcement officials will "request" ID cards from Asians, Blacks or Hispanic American citizens or resident aliens to make sure that they are "legal" -- simply because they look "foreign".

As such, the Organization of Chinese Americans unequivocally opposes the creation of a national ID card and will continue to do so. The creation of a national ID card -- or any form of a standardized national identification system -- is highly repugnant morally, ethically as well as constitutionally. Reducing each person to a number makes a travesty of the ideals of freedom, choice and individuality that the United States is founded upon.

EDWARD R. ROYBAL
25th District, California

2211 Rayburn Office Building
Washington, DC 20515
Telephone: (202) 225-6235

LOS ANGELES OFFICE:
Room 7106, New Federal P.O. Bldg.
300 N. Los Angeles Street
Los Angeles, CA 90012
Telephone: (213) 894-4870

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEE ON APPROPRIATIONS
CHAIRMAN,
SUBCOMMITTEE ON
TREASURY-POSTAL SERVICE-
GENERAL GOVERNMENT
MEMBER,
SUBCOMMITTEE ON
LABOR-HEALTH AND HUMAN
SERVICES-EDUCATION

CHAIRMAN,
SELECT COMMITTEE ON AGING

CHAIRMAN,
SUBCOMMITTEE ON
RETIREMENT INCOME
AND EMPLOYMENT

STATEMENT OF THE HONORABLE EDWARD R. ROYBAL (D-CA) MEMBER OF CONGRESS BEFORE THE WAYS AND MEANS SUBCOMMITTEE ON SOCIAL SECURITY

FEBRUARY 27, 1991

Mr. Chairman:

Thank you for allowing me this opportunity to testify before your subcommittee today.

The issue before us today is whether the United States should establish a form of national I.D. card which all Americans must possess. National I.D. cards are a favorite tool of totalitarian governments around the world. I fear that a national I.D. card could be the first step in restricting the movement and activities of the American people, and create fear and suspicion within many segments of our society.

When the social security card system was set up during the Great Depression, it was feared that the social security card number might become a national identification number. Although the government at first expressed that social security numbers were only to be used for social security purposes, today we must provide our social security number for tasks as diverse as opening a bank account or writing a check at the grocery store. It is inevitable that if a national I.D. card system were set up in America today, we would soon see the card being used for non-intended purposes such as checking a person's credit history.

It is also clear that a national I.D. card would lead to discrimination against ethnic and racial minorities. Last year, the General Accounting Office released a report which documented widespread discrimination by employers against foreign-looking and foreign-sounding job applicants. If a national I.D. card were established, it is obvious that people who look "foreign" would be much more likely to be asked to show it. The specter of brown-skinned Americans being asked to show their "national I.D. card" by authorities brings to mind unsavory images similar to those in South Africa under the hated pass-card system.

If a national I.D. card system is imposed upon this country, ethnic and racial minorities across the United States are much more likely than other groups to feel the brunt of discrimination. Some proponents of a national I.D. card system have put forth the claim that a card used only for employment and hiring purposes would be an effective tool for combatting terrorism. I cannot comprehend why a terrorist who illegally enters this country would seek employment before committing a terrorist act.

In conclusion, let me reiterate that the establishment of a national I.D. card system, whether under the purview of the Social Security Administration or some other government agency, would infringe upon the civil rights and civil liberties which Americans now enjoy and lead to increased intrusions into people's private matters.

Thank you for allowing me this time.

STATEMENT OF HON. ESTEBAN E. TORRES, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Chairman Jacobs and members of the subcommittee, I would first like to thank you for calling this hearing today to discuss the implications of the use of the social security number as a national identifier.

Let me share with you my own personal experience with the use of a national identifier. When I was priviledged to serve as this nation's ambassador to UNESCO in Paris my children were required to have on their person, at all times, an identification card issued by the government of France.

My young son, Steve, with his long curly hair and olive skin, looked more like someone from Algeria or a Middle Eastern country than an American. He was constantly stopped by the police and questioned.

One day he left our house without his I.D. card and was picked up by the police and thrown in jail. When I went down to the station to secure his release, I vowed to myself and to my children that if I had it in my power, I would never let such a system take foot hold in the United States.

Mr. Chairman, I congratulate you for recognizing that a proposal for a national identifier should not reach the legislative floor without a hearing. Indeed, the necessity of a hearing is of paramount importance on this matter, given that the legislation proposed would have far-reaching effects on the quality of life of each and everyone of our citizens, and upon every aspect of their lives--both public and private.

The concept of a national identifier was most recently proposed without any hearings, as a last minute addition to necessary immigration legislation. It reached the legislative floor without the benefit of much-needed discussion. Yet, proposals with such pervasive effects on our nation's way of life must be openly discussed and thoroughly analyzed. Today's hearing is a beginning to that end.

The personal experience which I have related to you is an illustration of one of the effects of a system of national identification. Under the French system described, any citizen may be stopped at any time without the protection of due process or reasonable cause. French law holds that anyone who looks "suspicious" may be stopped and questioned for an identification card. If the person questioned cannot produce papers proving his identity, he or she may be held for up to four hours. This system bypasses protections which we, in this country, hold dear.

The establishment of a national identifier establishes a legal basis for a violation of civil rights such as I have described to you. It does so because it establishes a legal basis for government to control all aspects of the lives of its citizens. The establishment of such absolute power and control over individual citizens creates the potential for abuse of this power.

Under such a system all citizens are vulnerable to abuse of this power. However, those who "look different," those who who are not part of the main power structure of the society, who do not, in some way, conform with that power structure are the most vulnerable. Such vulnerable groups could include protestors or ethnic minorities. My son's experience underscores this vulnerability.

The creation of a national identifier system gives government the infrastructure necessary to become the Orwellian "Big Brother." It may enable a government to link information about our families, to information about our employement, to information about our credit history. Are we strong enough or wise enough or moral enough to cope with the kind of power we would amass? Does the demand for greater security and comfort, for greater efficiency, justify the substantial loss in personal freedoms that such control would permit? Those who appear "different" are the most vulnerable to this loss of freedom.

Let us all be aware of the tremendous irony of the matter we have before us. The governement of South Africa, after years of struggle, just abolished identifier pass books that were used to discriminate against its black citizens. Ironically, at the same time, the United States considers taking the idea up.

○